System Administrator Guide to the Criterions EHR

Security

While the Criterions EHR is a client/server based product with a browser based interface, some clients choose to allow access across public networks (i.e. the Internet) to provide remote access.

While this increases level of functionality in some cases, this also presents security risks to your data, your practice, and ultimately, your patients.

Criterions, LLC. formally requires all clients to adhere to security measures if attempting to access data across open networks.

	Security of practice and patient information is the sole responsibility of the practice. Guidelines given below may or may not apply to any given practice and are for information purposes only. A system administrator should perform a vetting of client needs and make appropriate recommendations.

If you have questions or need assistance is configuring your network to meet security standards, please contact Criterions at 516.466.1942 or info@criterions.com

Contents

Security 2
Overview 5
Remote Access 5
1.0 - Windows Domain Authentication 5
Configuring Windows Authentication 6
2.0 - SSL 20
IIS 6.0 20
Verify that SSL is working 30
4.0 - Password Transfer 32
5.0 – Power Supply 33
6.0 – Network/System Requirements 33
7.0 – HL7 – Electronic Lab Retrieval 36
8.0 – Electronic Billing 36
9.0 – Peripherals – Printing, Scanning, Faxing, Email 37
Setting Up eRx Printing Alignment 37
10.0 – Updates to System 41
TCMS 41
EHR 42
11.0 – Error Logs 44
Common System Error Messages 45
Navigation Errors 46
12.0 – EHR User and Practice Setup 49
13.0 – System Backup 53
14.0 – Remote Support 57
15.0 – User Setup, Rights, Passwords and Audits 60

15.1 – Accessing Setup 60
Create a User Group 61
Modify Existing User Accounts 69
Deactivate a User Account 73
Passwords 83
Admin Reset of Passwords 88
Administrative Unlocking of Accounts 95
Incorrect User Attempts 101
Accessing Audit Logs 104
Contact 120

Overview

The following document contains guidelines a system administrator should adhere to when developing a network for a practice. These are security and network settings that provided a heightened level of security to data and systems while allowing access to authorized users.

	Note: This document contains guidelines for practices to follow. The client system administrator should perform a thorough vetting process to determine client needs and configure the system accordingly, complying with all regulations and security standards.

Remote Access

	If deemed acceptable by the systems administrator, the application can be made available over https via the internet. Client must authenticate themselves against the application using their secure login. If the server resides on a domain the network administrator may choose to require the user authenticate against the domain in addition to the application.

1.0 - Windows Domain Authentication

Windows authentication without impersonation. This is the default setting. ASP.NET performs operations and accesses resources by using your application's process identity, which by default is the Network Service account on Windows Server 2003.

URL authorization. You use URL authorization to control access to requested files and folders based on the request URL. You configure URL authorization by using an <**authorization**> element in the Web.config file to control which users and groups of users should have access to requested resources. Authorization is based on the **IPrincipal** object stored in **HttpContext.User**. With Windows authentication, this object is of type **WindowsPrincipal** and it contains a **WindowsIdentity** object that holds the Windows token for the authenticated user.

Note ASP.NET version 2.0 on Windows Server 2003 protects all files in a particular directory, even those not mapped to ASP.NET such as .html, .gif, and .jpg files.

Configuring Windows Authentication

To configure your application to use Integrated Windows authentication, you must use IIS Manager to configure your application's virtual directory security settings and you must configure the <**authentication**> element in the Web.config file.

To configure Windows authentication

1. Start Internet Information Services (IIS).
2. Right-click your application's virtual directory, and then click **Properties**.
3. Click the **Directory Security** tab.
4. Under **Anonymous access and authentication control**, click **Edit**.
5. Make sure the **Anonymous access** check box is not selected and that **Integrated Windows authentication** is the only selected check box.

In your application's Web.config file or in the machine-level Web.config file, ensure that the authentication mode is set to Windows as shown here.

Windows Server 2003 includes all the functionality customers expect from a mission critical Windows Server operating system, such as security, reliability, availability, and scalability. In addition, Microsoft has improved and extended the Windows server product family to enable organizations to experience the benefits of Microsoft .NET—a set of software for connecting information, people, systems, and devices.

This tutorial will explain how to create a first domain controller(DC) in your network or company includes DNS server setup in windows server 2003 .You have to install DNS server for DC without DNS the client computers wouldn't know which one is DC.You can host DNS on a different server than DC.

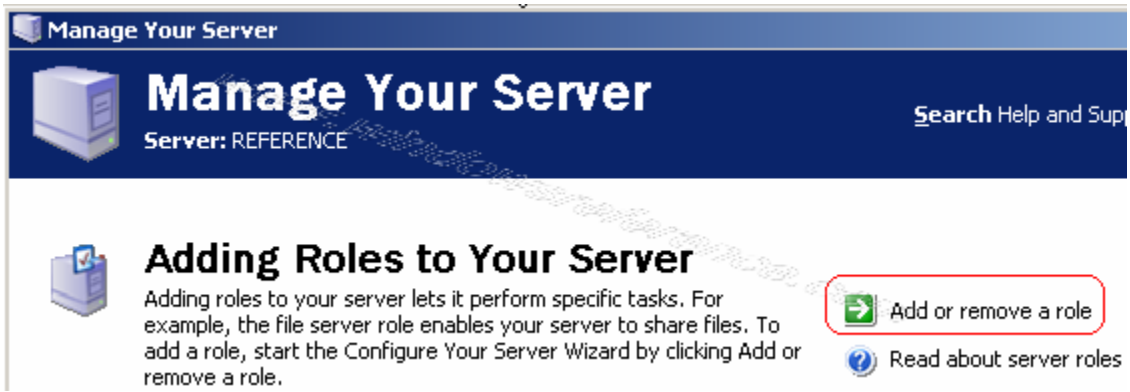
Before Starting the DC installation process you need to make sure the following points

- You have installed Basic windows server 2003 installation
- Make sure you have assigned a static ip address to your server

Now start DC and DNS Setup process

1. First you need to go to Start–>All Programs–>Administrative Tools–>Manage Your Server

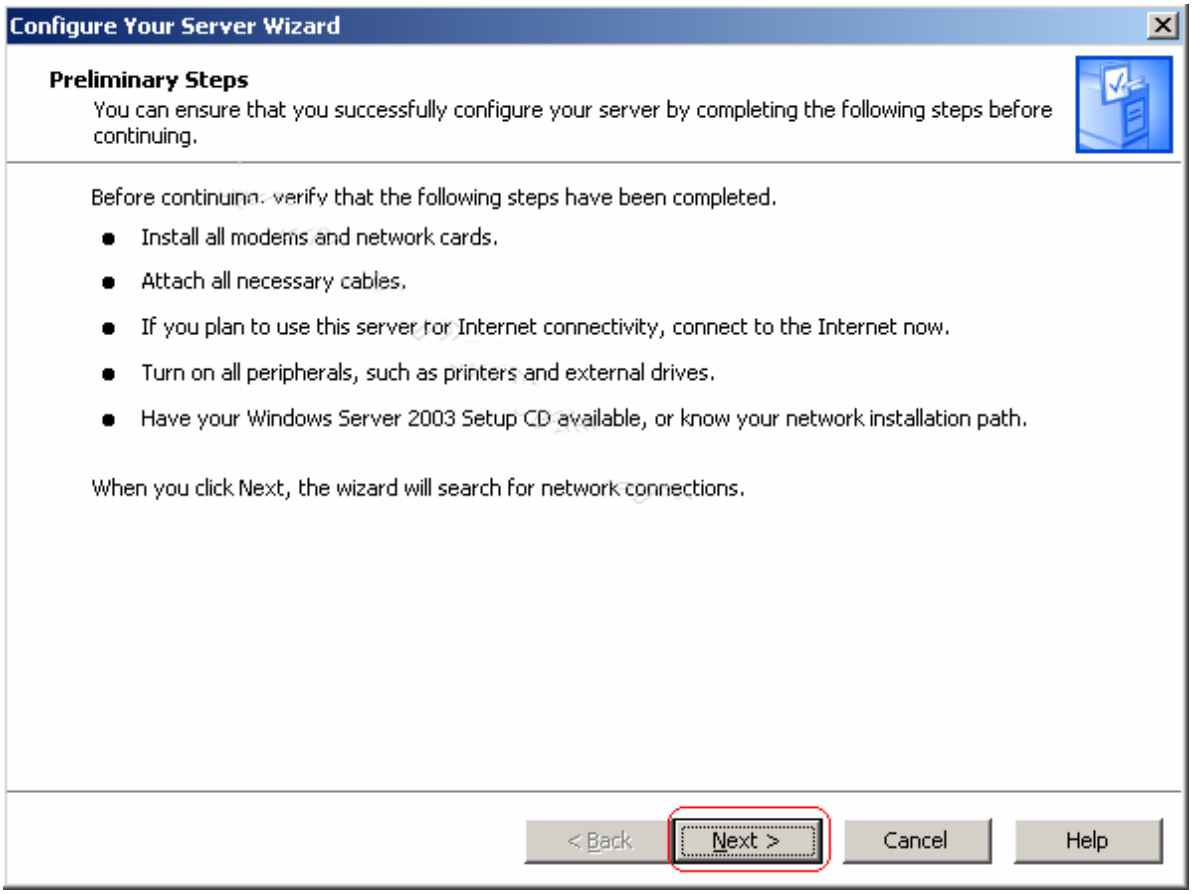
Here you need to select Add or remove a role.


Manage Your Server
Manage Your Server
Server: REFERENCE
Search Help and Sup
Adding Roles to Your Server
Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role.
Add or remove a role
Read about server roles

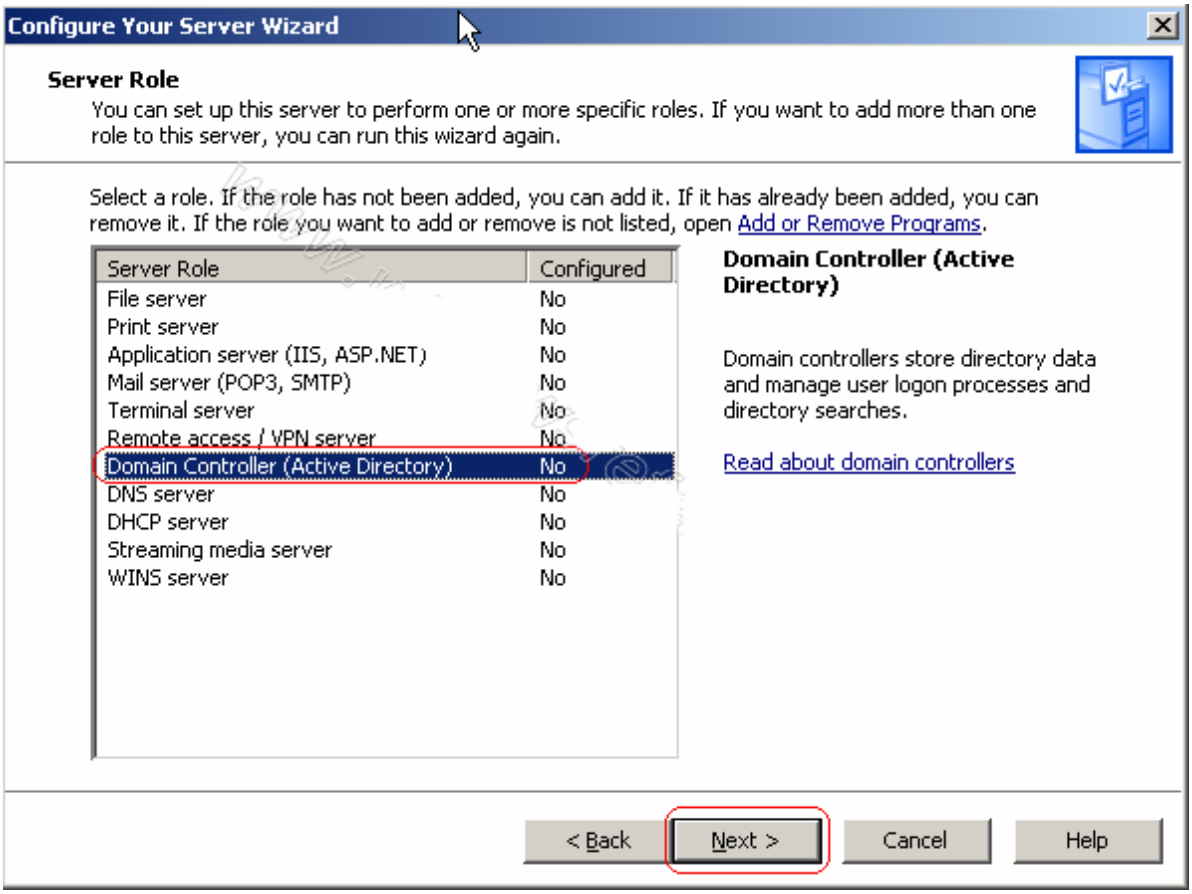
2. Click Add or remove a role.

Verify the following steps.

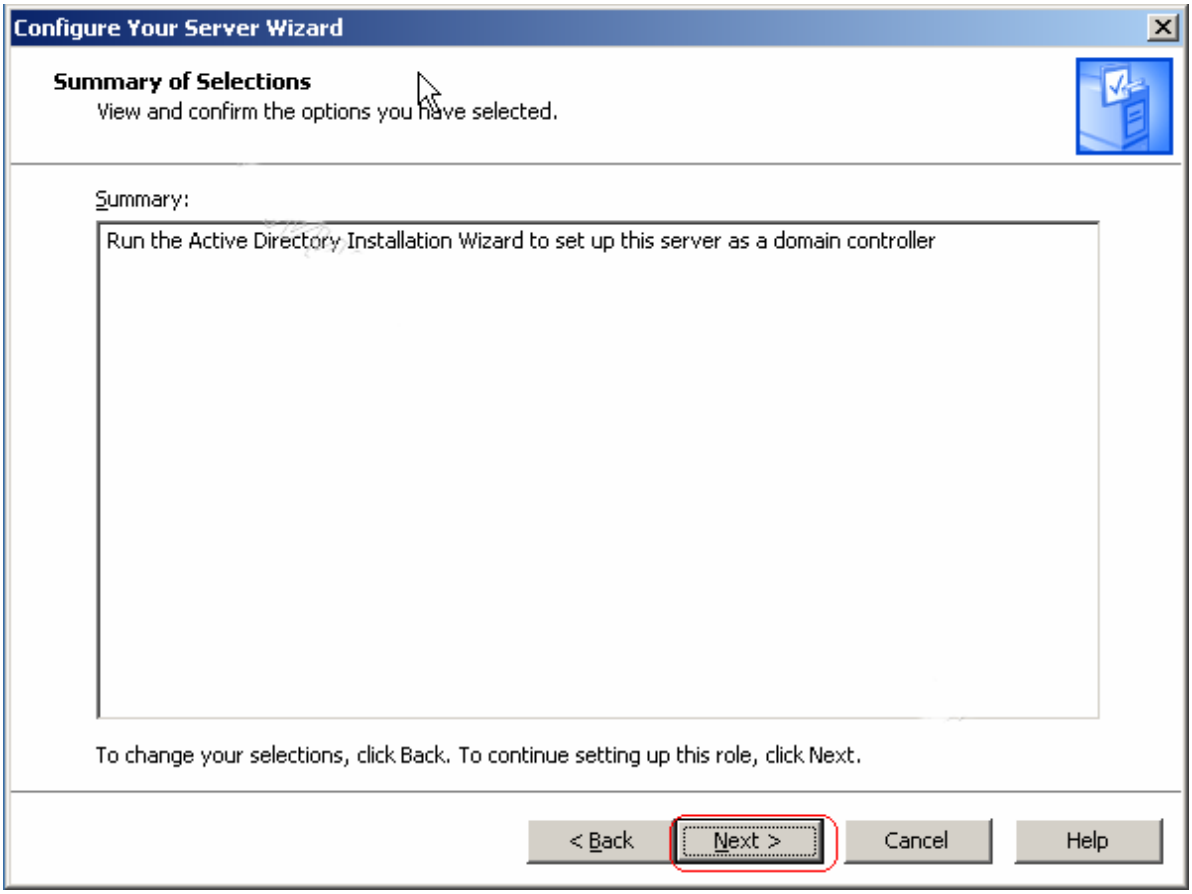
3. Click on Next


Configure Your Server Wizard
Preliminary Steps
You can ensure that you successfully configure your server by completing the following steps before continuing.
Before continuing, verify that the following steps have been completed.
Install all modems and network cards.
Attach all necessary cables.
If you plan to use this server for Internet connectivity, connect to the Internet now.
Turn on all peripherals, such as printers and external drives.
Have your Windows Server 2003 Setup CD available, or know your network installation path.
When you click Next, the wizard will search for network connections.
< Back
Next >
Cancel
Help

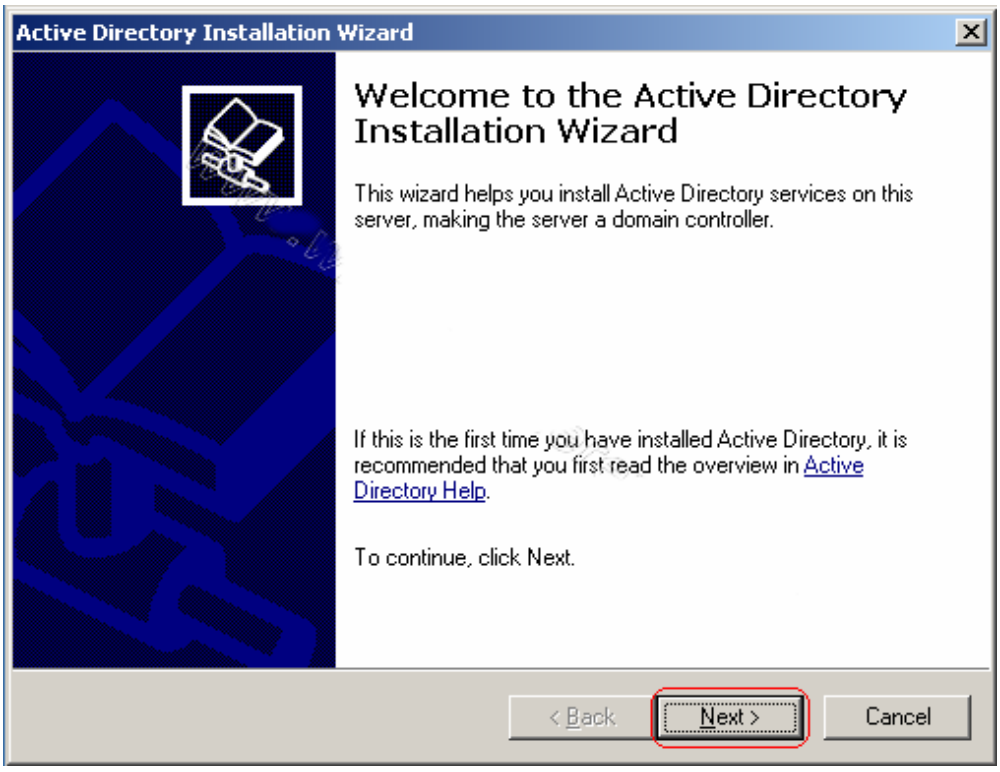
4. Select Server Role as Domain Controller option click on Next.


Configure Your Server Wizard
Server Role
You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.
Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open Add or Remove Programs.
Server Role
Configured
File server No
Print server No
Application server (IIS, ASP.NET) No
Mail server (POP3, SMTP) No
Terminal server No
Remote access / VPN server No
Domain Controller (Active Directory) No
DNS server No
DHCP server No
Streaming media server No
WINS server No
Domain Controller (Active Directory)
Domain controllers store directory data and manage user logon processes and directory searches.
Read about domain controllers
< Back
Next >
Cancel
Help

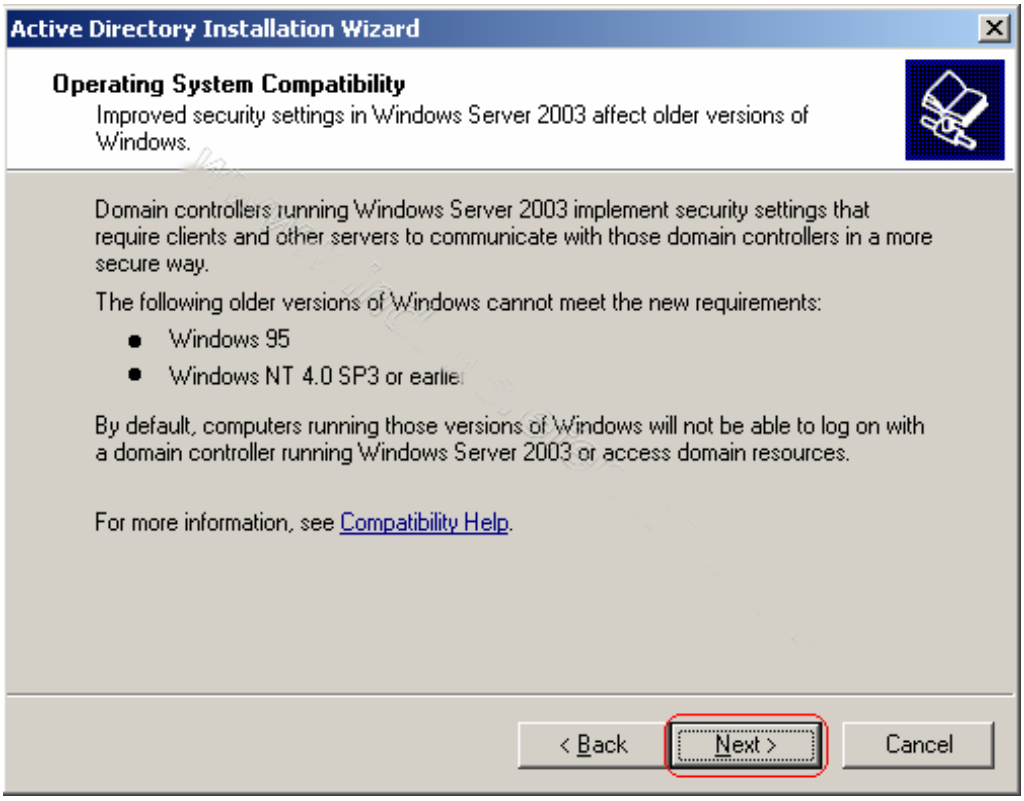
5. Summary of Your Selections click on Next.


Configure Your Server Wizard
Summary of Selections
View and confirm the options you have selected.
Summary:
Run the Active Directory Installation Wizard to set up this server as a domain controller
To change your selections, click Back. To continue setting up this role, click Next.
< Back
Next >
Cancel
Help

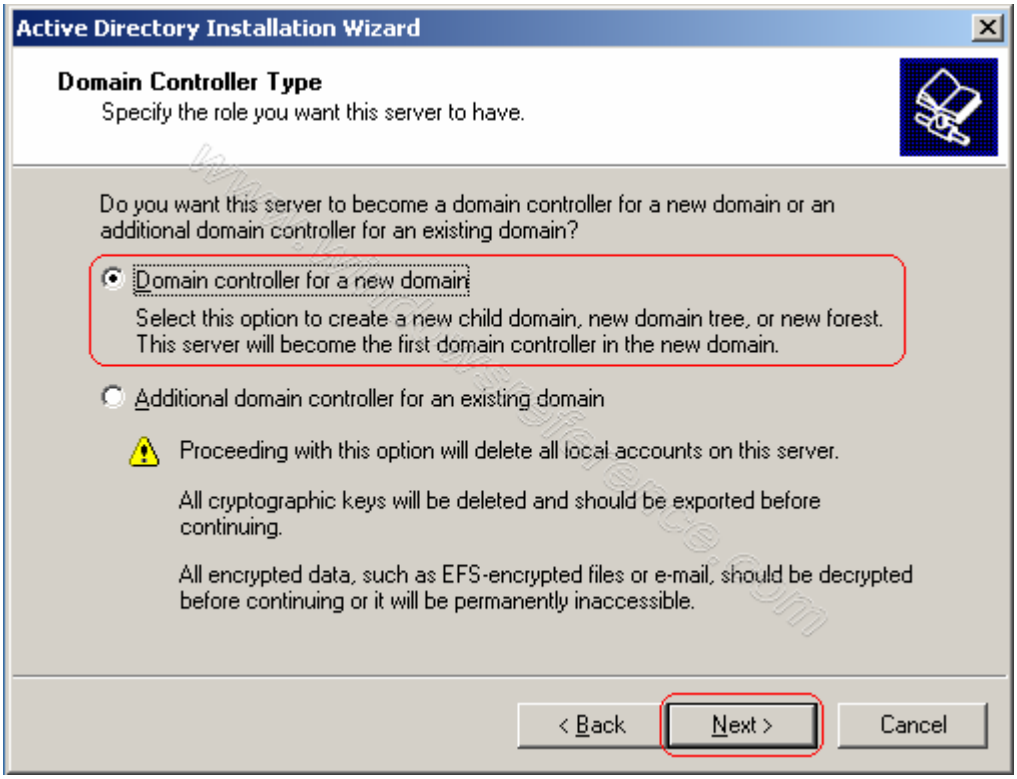
6. Active Directory Installation Wizard click on Next.


Active Directory Installation Wizard
Welcome to the Active Directory Installation Wizard
This wizard helps you install Active Directory services on this server, making the server a domain controller.
If this is the first time you have installed Active Directory, it is recommended that you first read the overview in Active Directory Help.
To continue, click Next.
< Back
Next >
Cancel

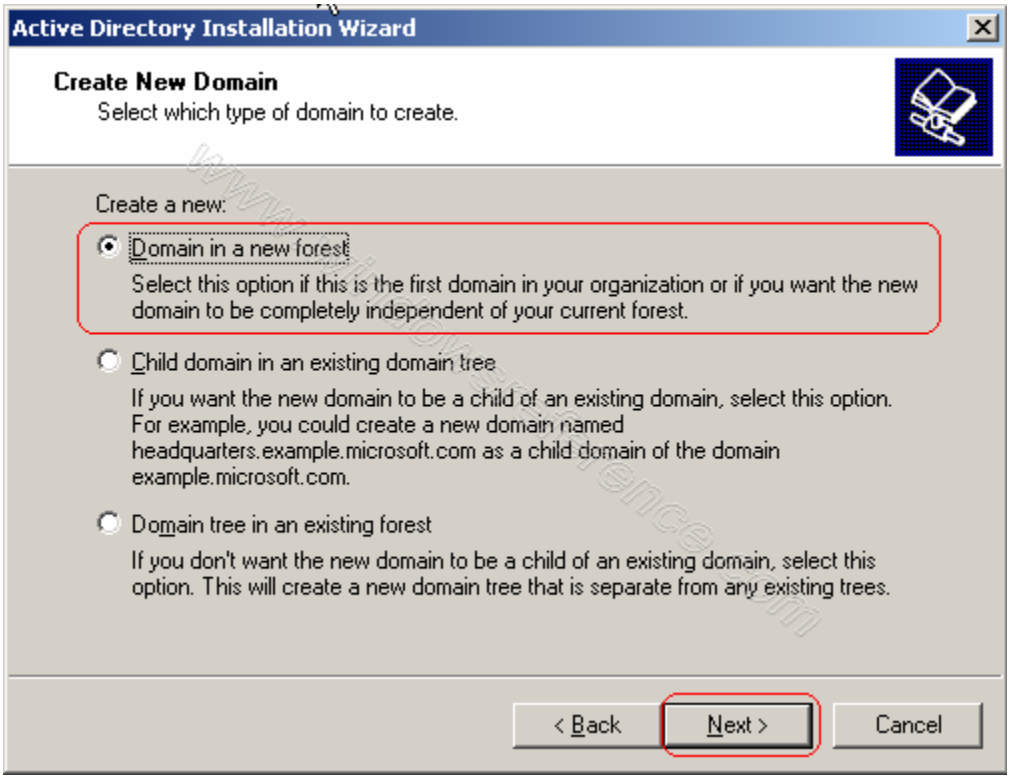
7. Click “Next” on the compatibility window.


Active Directory Installation Wizard
Operating System Compatibility
Improved security settings in Windows Server 2003 affect older versions of Windows.
Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
The following older versions of Windows cannot meet the new requirements:
Windows 95
Windows NT 4.0 SP3 or earlier
By default, computers running those versions of Windows will not be able to log on with a domain controller running Windows Server 2003 or access domain resources.
For more information, see Compatibility Help.
< Back
Next >
Cancel

8. Next window select the default option of “Domain Controller for a new domain” and click “Next”.

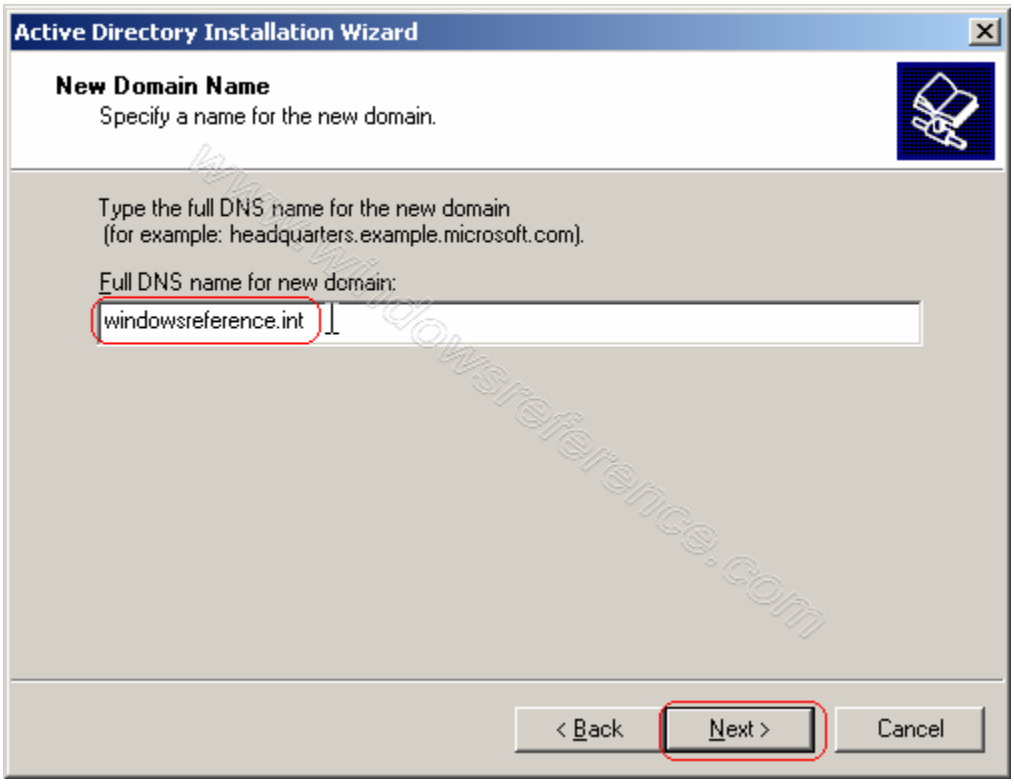

Active Directory Installation Wizard
Domain Controller Type
Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< Back
Next >
Cancel

9. In this tutorial we will create a domain in a new forest, because it is the first DC, so keep that option selected.

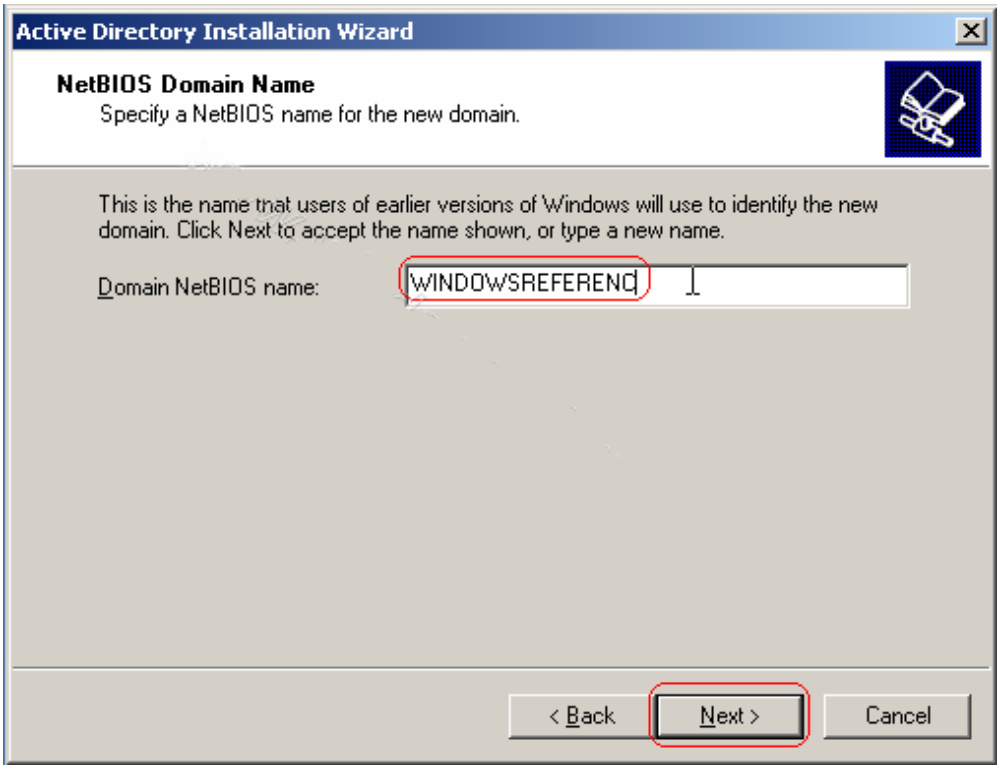

Active Directory Installation Wizard
Create New Domain
Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< Back
Next >
Cancel

Now we have to think of a name for our domain. If you have a domain like “criterions.com”, you can use it, but it isn’t suggested because computers inside of your domain may not be able to reach the company website. Active directory domains don’t need to be “real” domains like the one above - they can be anything you wish.

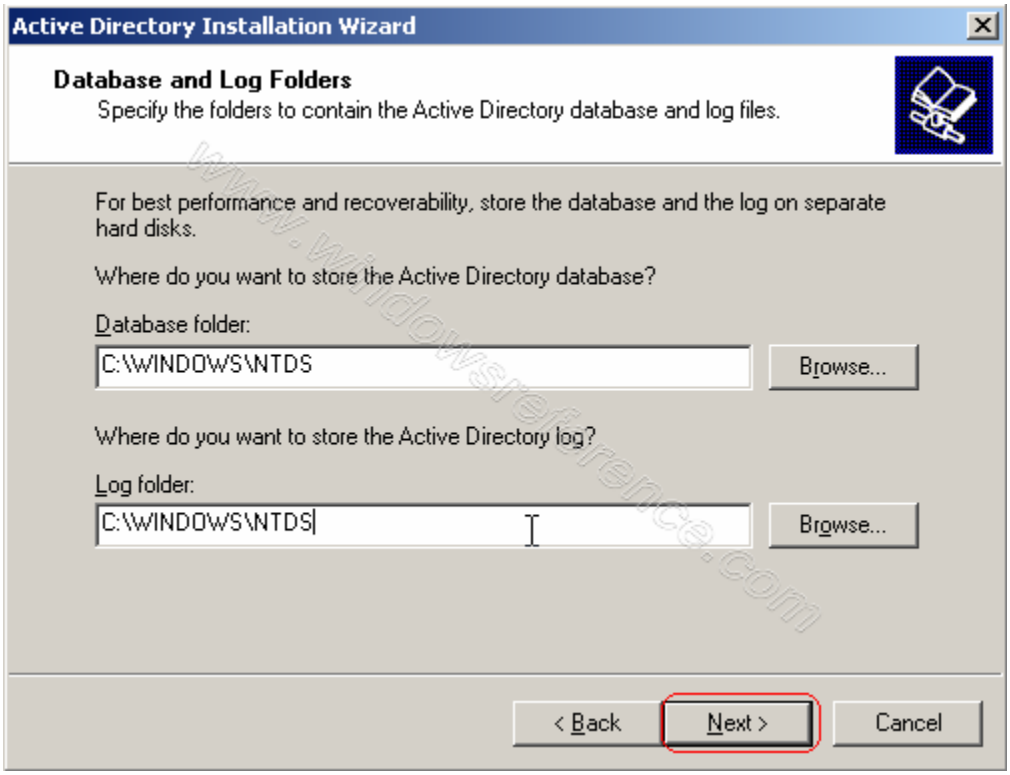
Example: “internaldomain.int”.


Active Directory Installation Wizard
New Domain Name
Specify a name for the new domain.
Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).
Full DNS name for new domain:
windowsreference.int
< Back
Next >
Cancel

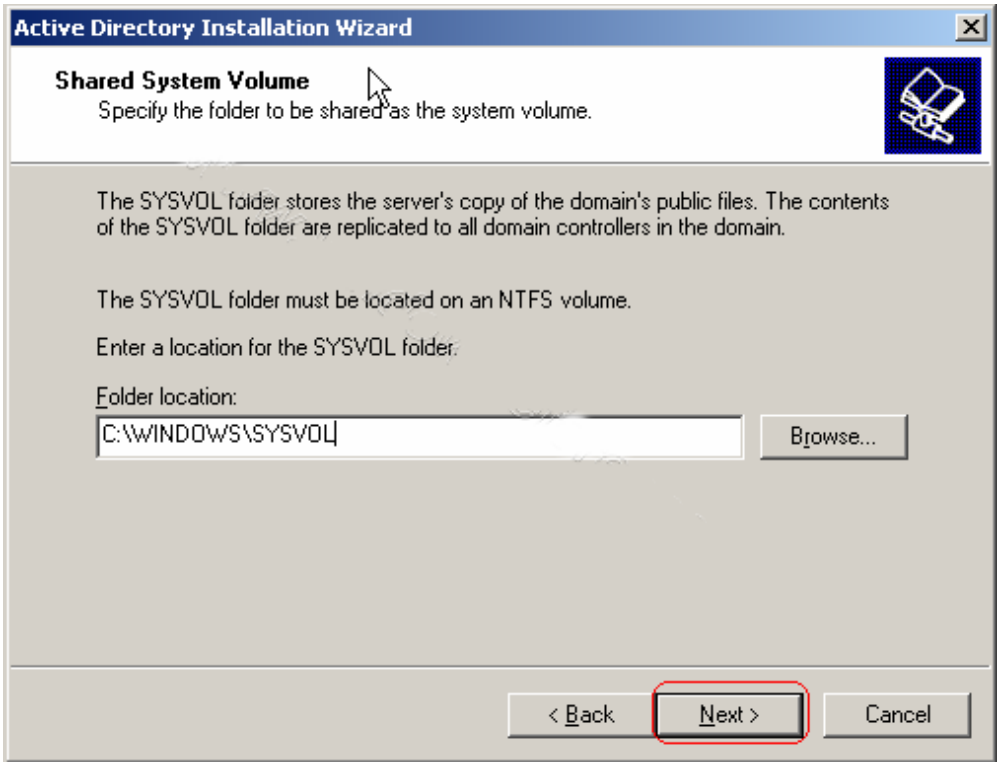
Now in order to keep things simple, we will use “windowsreferenc”, which is the default selection, as the NetBIOS name of the domain.


Active Directory Installation Wizard
NetBIOS Domain Name
Specify a NetBIOS name for the new domain.
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.
Domain NetBIOS name:
WINDOWSREFERENC
< Back
Next >
Cancel

The next dialog suggests storing the AD database and log on separate hard disks and you can just leave the default settings.


Active Directory Installation Wizard
Database and Log Folders
Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:\WINDOWS\NTDS
Browse...
Where do you want to store the Active Directory log?
Log folder:
C:\WINDOWS\NTDS
Browse...
< Back
Next >
Cancel

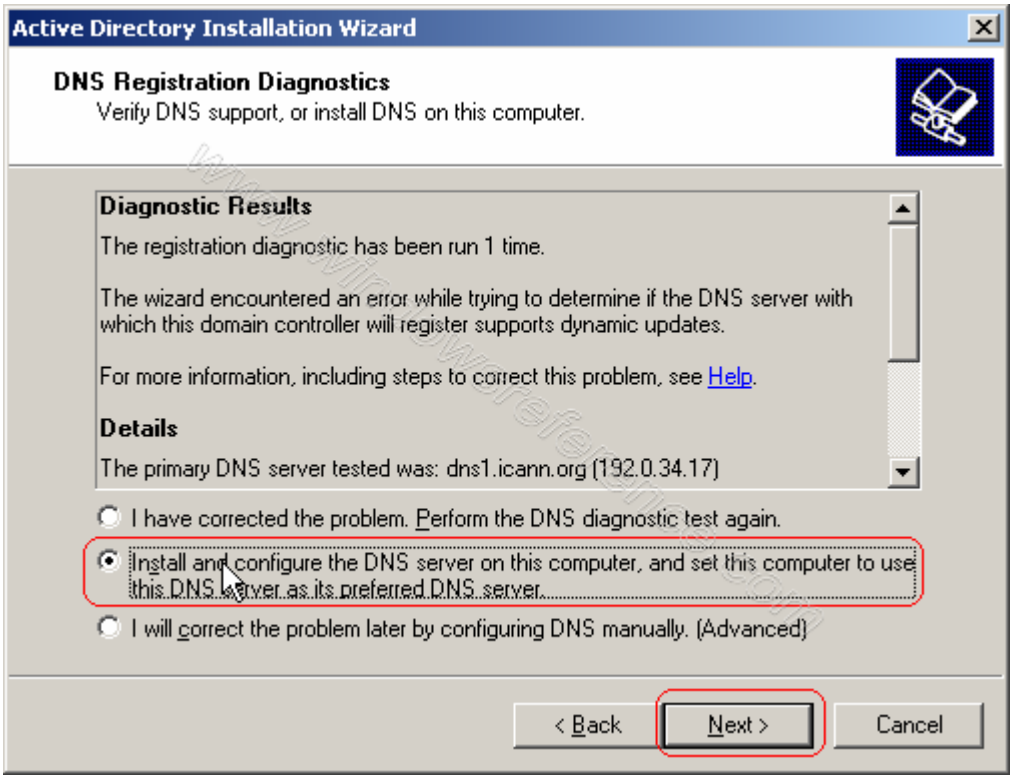
The SYSVOL folder is a public share, where things like .MSI software packages can be kept when you will distribute packages and you can just leave the default settings or you can change the path.


Active Directory Installation Wizard
Shared System Volume
Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Folder location:
C:\WINDOWS\SYSVOL
Browse...
< Back
Next >
Cancel

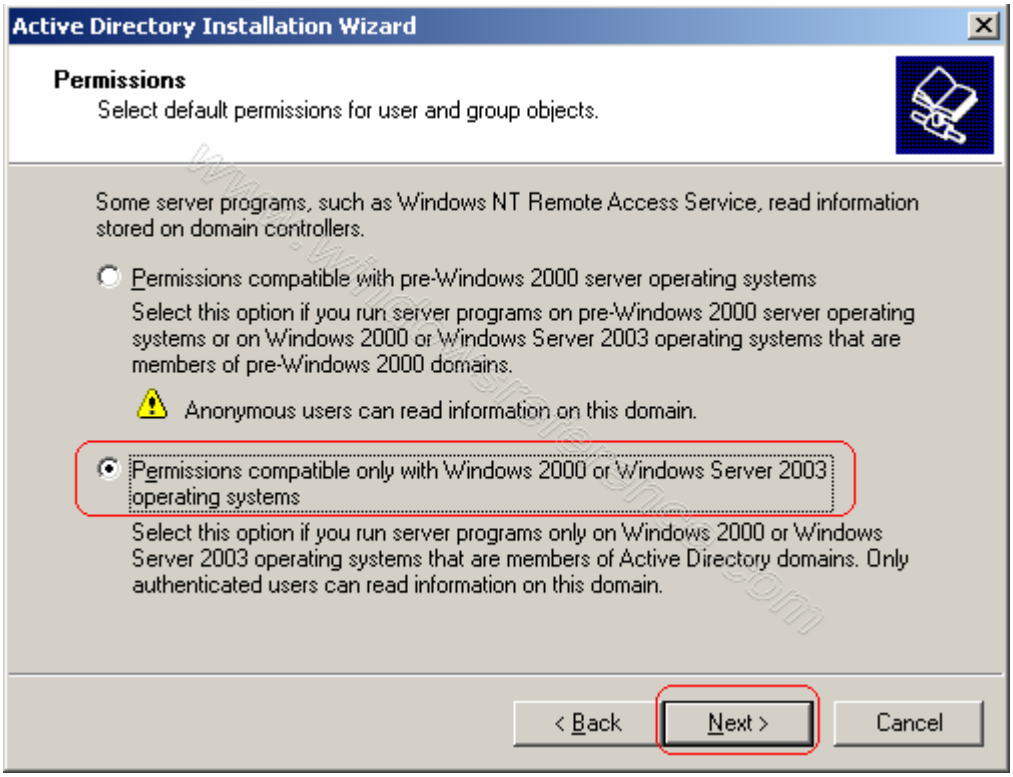
Next Screen basically says that you will need a DNS server in order for everything to work the way we want it (i.e., our “windowsreference.int” to be reachable).

Install the DNS server on this machine or if you want you can installed else where.

10. Select “Install and Configure…” and click Next.

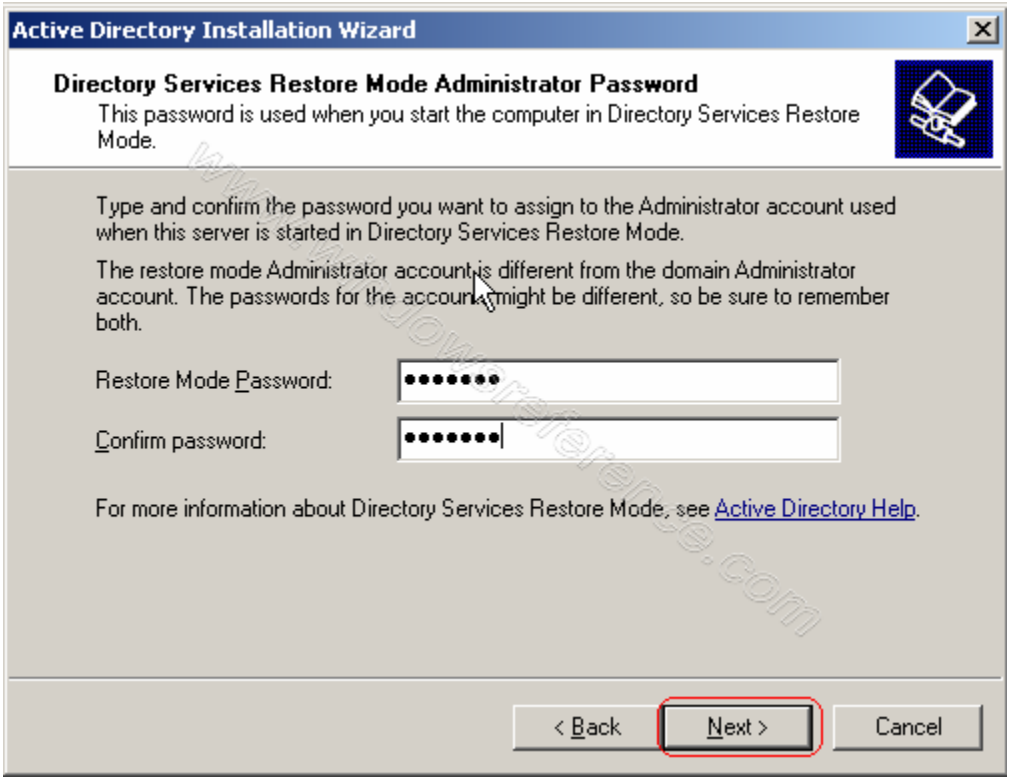

Active Directory Installation Wizard
DNS Registration Diagnostics
Verify DNS support, or install DNS on this computer.
Diagnostic Results
The registration diagnostic has been run 1 time.
The wizard encountered an error while trying to determine if the DNS server with which this domain controller will register supports dynamic updates.
For more information, including steps to correct this problem, see Help.
Details
The primary DNS server tested was: dns1.icann.org (192.0.34.17)
I have corrected the problem. Perform the DNS diagnostic test again.
Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.
I will correct the problem later by configuring DNS manually. (Advanced)
< Back
Next >
Cancel

11. Here you need to select the permissions for win 2000 or win 2003 server if you have any NT4 select first option otherwise select second option and click Next.


Active Directory Installation Wizard
Permissions
Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 server operating systems
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain.
Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.
< Back
Next >
Cancel

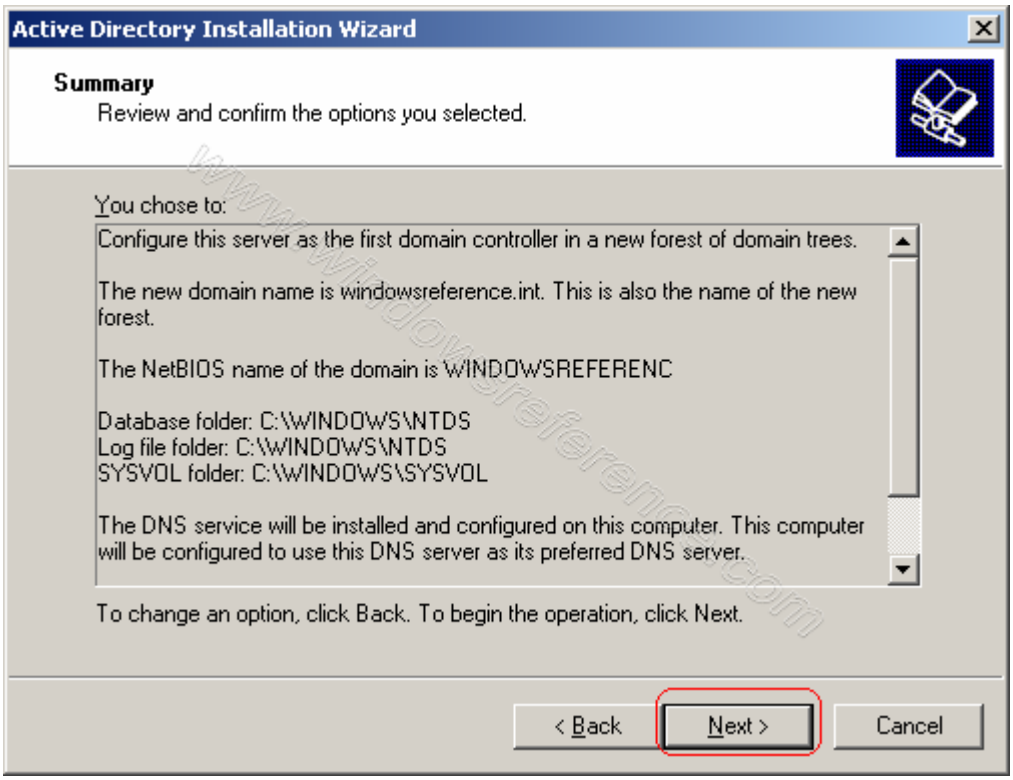
The restore mode password is the single password that all administrators hope to never use, however they should also never forget it because this is the single password that might save a failed server.

12. Click Next.

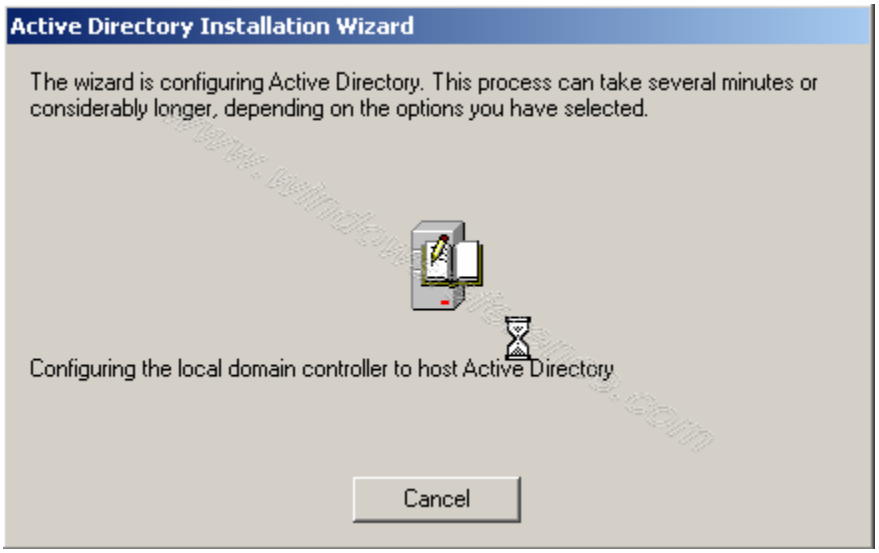

Active Directory Installation Wizard
Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.
Restore Mode Password:
Confirm password:
For more information about Directory Services Restore Mode, see Active Directory Help.
< Back
Next >
Cancel

Now we will see a summary of what will happen.

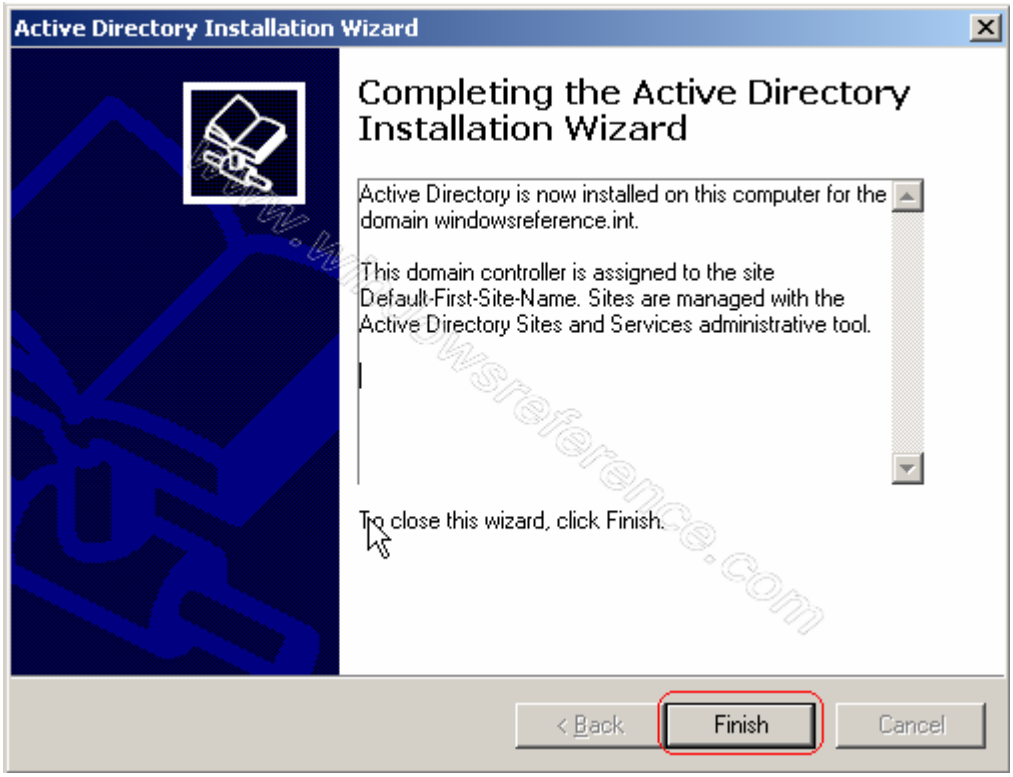
13. Click Next.


Active Directory Installation Wizard
Summary
Review and confirm the options you selected.
You chose to:
Configure this server as the first domain controller in a new forest of domain trees.
The new domain name is windowsreference.int. This is also the name of the new forest.
The NetBIOS name of the domain is WINDOWSREFERENC
Database folder: C:\WINDOWS\NTDS
Log file folder: C:\WINDOWS\NTDS
SYSVOL folder: C:\WINDOWS\SYSVOL
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.
To change an option, click Back. To begin the operation, click Next.
< Back
Next >
Cancel

Active directory installation process started this can take several minutes. It's likely that you will be prompted for your Windows Server 2003 CD (for DNS) so have it handy.


Active Directory Installation Wizard
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.
Configuring the local domain controller to host Active Directory
Cancel

14. Active directory Installation finish screen click Finish.

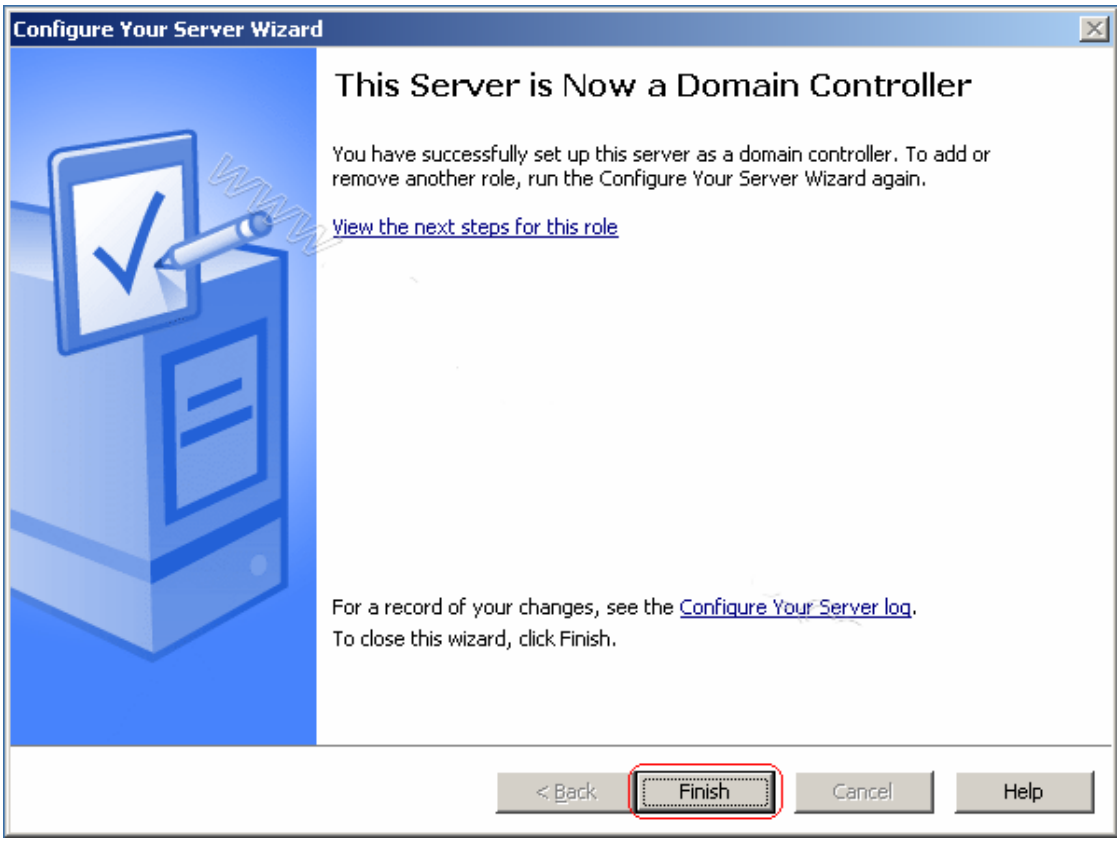

Active Directory Installation Wizard
Completing the Active Directory Installation Wizard
Active Directory is now installed on this computer for the domain windowsreference.int.
This domain controller is assigned to the site Default-First-Site-Name. Sites are managed with the Active Directory Sites and Services administrative tool.
To close this wizard, click Finish.
< Back
Finish
Cancel

15. Now you need to select “Restart Now” option to reboot your server.

Active Directory Installation Wizard
Windows must be restarted before the changes made by the Active Directory Installation wizard take effect.
Restart Now
Don't Restart Now

After rebooting you can see new option for logon

After logging in you can see similar to the following screen saying your server is now domain controller.


Configure Your Server Wizard
This Server is Now a Domain Controller
You have successfully set up this server as a domain controller. To add or remove another role, run the Configure Your Server Wizard again.
View the next steps for this role
For a record of your changes, see the Configure Your Server log.
To close this wizard, click Finish.
< Back
Finish
Cancel
Help

That's it now your server is configured as domain controller and DNS server.

2.0 - SSL

Secure Socket Layer (SSL) is a protocol to provide security and data integrity across open networks. SSL functions by not only verifying the servers authenticity, but also verifying the authenticity of the requesting party.

Using SSL requires a certificate to be purchased. Criterions, LLC will purchase and provide you with a certificate at your request.

Client are to disable access over HTTP protocol forcing all transaction to take place over HTTPS secure protocol. SSL properties are managed by both MS IIS and Router properties.

IIS 6.0

To configure SSL for your website on IIS 6.0 (running on Windows Server 2003) complete the following steps:

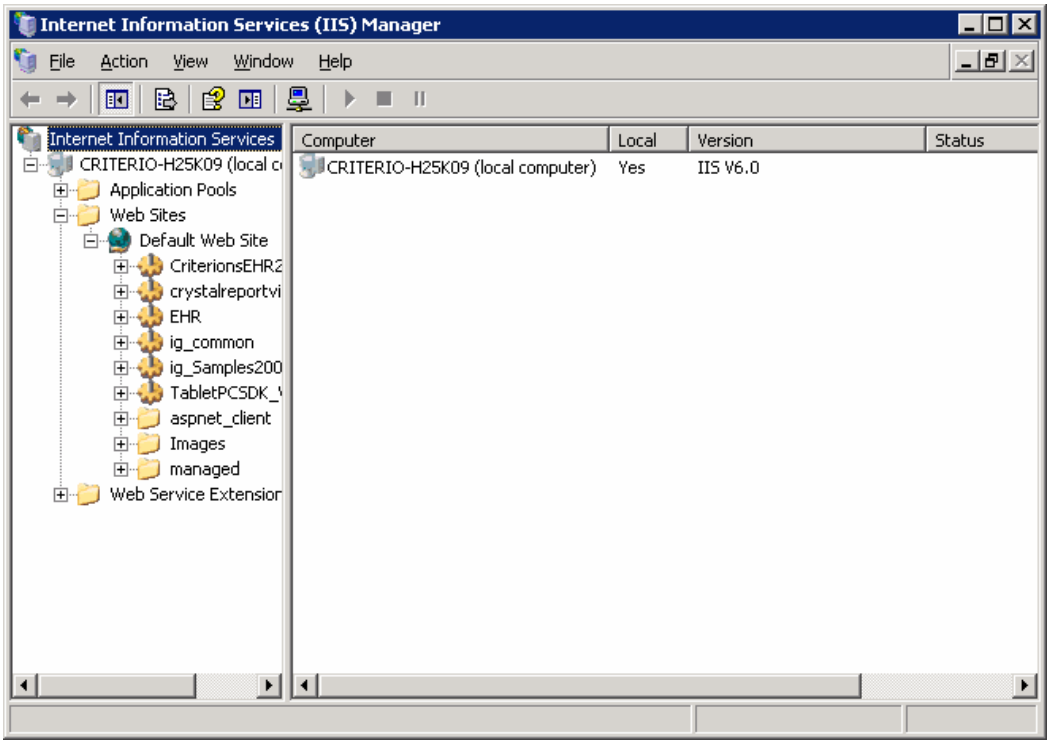
Note: Although the screenshots are made with IIS 6.0 on Windows Server 2003, the same procedure applies for IIS 5.0 and IIS 5.1.

1. Click Start, point to All Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. In Internet Services Manager, in the console tree, expand *SERVERNAME* (your local computer), and then expand Web Sites.
3. In the console tree, right-click Default Web Site, and then click Properties.

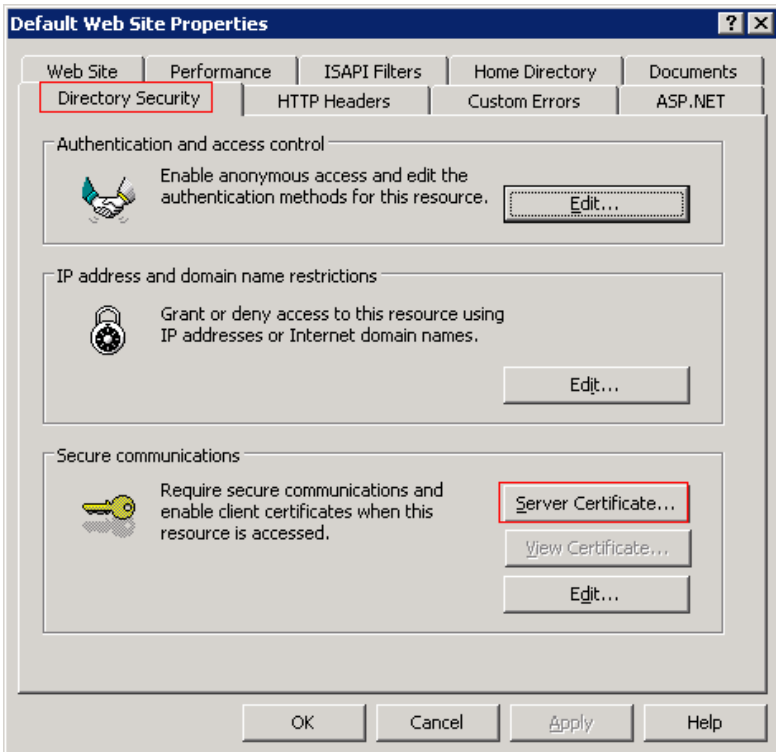
Note: It's possible that the site you've created was stored under a different virtual server. If your website is not stored within the Default Web Site, right-click your own web site and click Properties.

Part 1: Preparing a Certificate Request

Open the *Internet Information Services (IIS) Manager* (found in the Administrative Tools portion of the Control Panel).



Select the Website you wish to generate the certificate for, in this case, we will be using the *Default Website*. Right click and select properties.

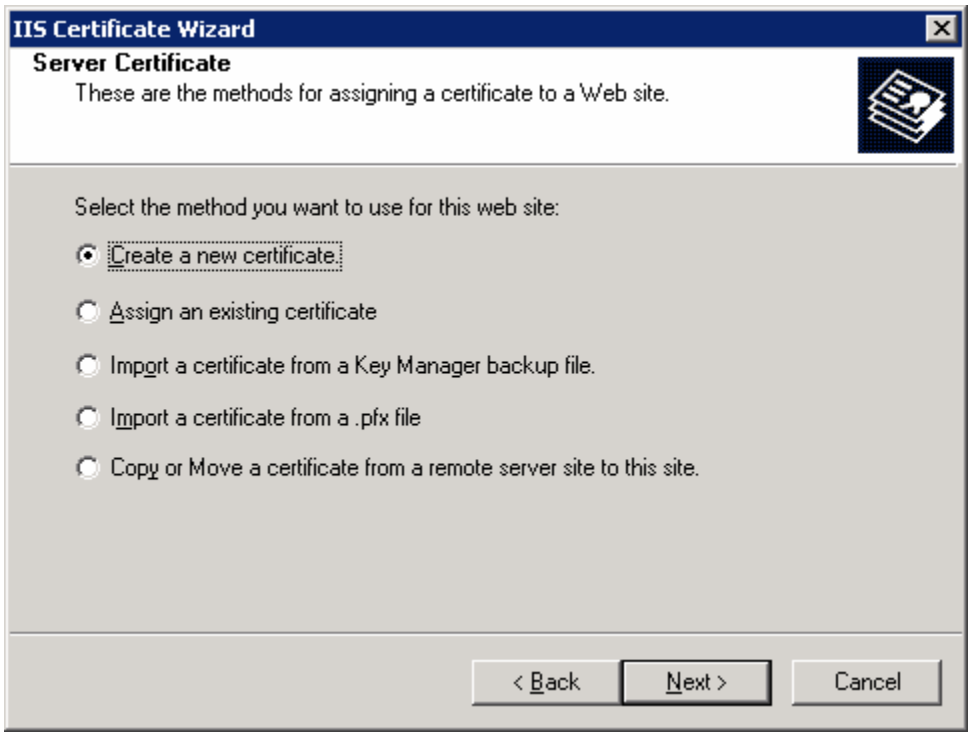


In the *Default Web Site Properties* window, select the 'Directory Security' tab and click on the 'Server Certificate' button to spawn the Web Server Certificate Wizard.

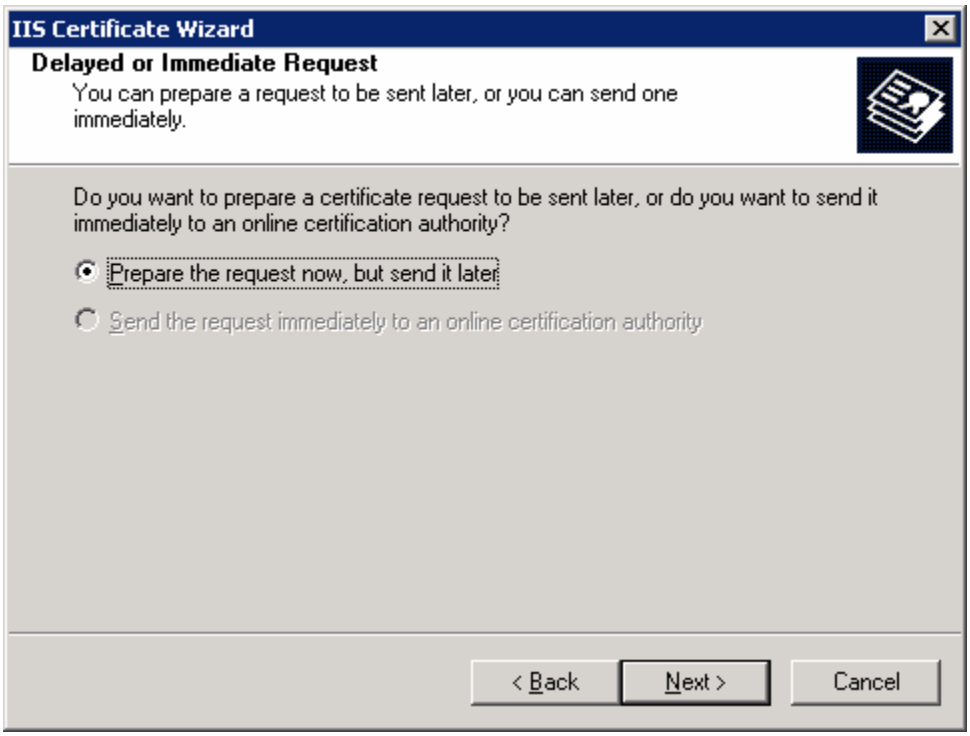
Click 'Next ' to advance beyond the introductory form:

Welcome to the Web Server Certificate Wizard.
Welcome to the Web Server Certificate Wizard
This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.
Status of your Web Server:
Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.
To continue, click Next.
< Back
Next >
Cancel

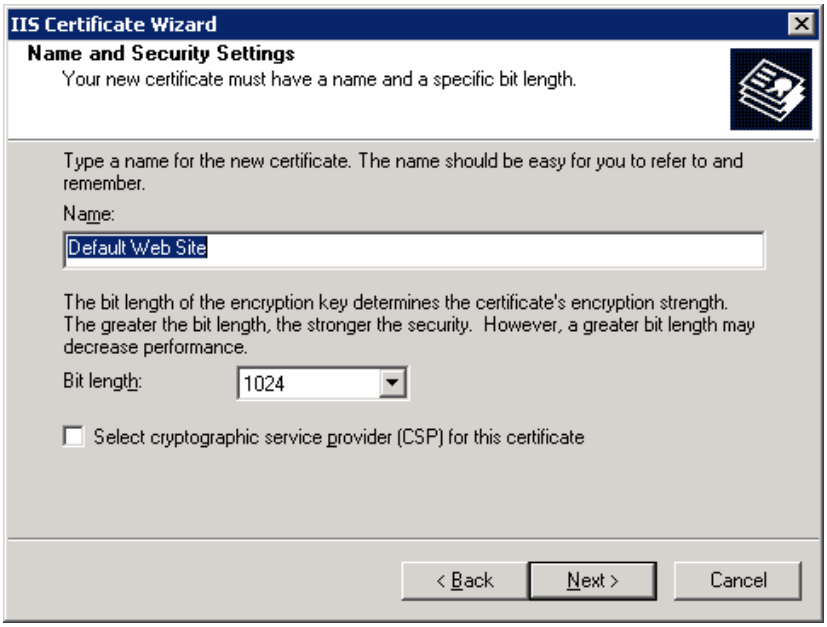
Select the first option 'Create a new Certificate' and click 'Next'.


IIS Certificate Wizard
Server Certificate
These are the methods for assigning a certificate to a Web site.
Select the method you want to use for this web site:
Create a new certificate.
Assign an existing certificate
Import a certificate from a Key Manager backup file.
Import a certificate from a .pfx file
Copy or Move a certificate from a remote server site to this site.
< Back
Next >
Cancel

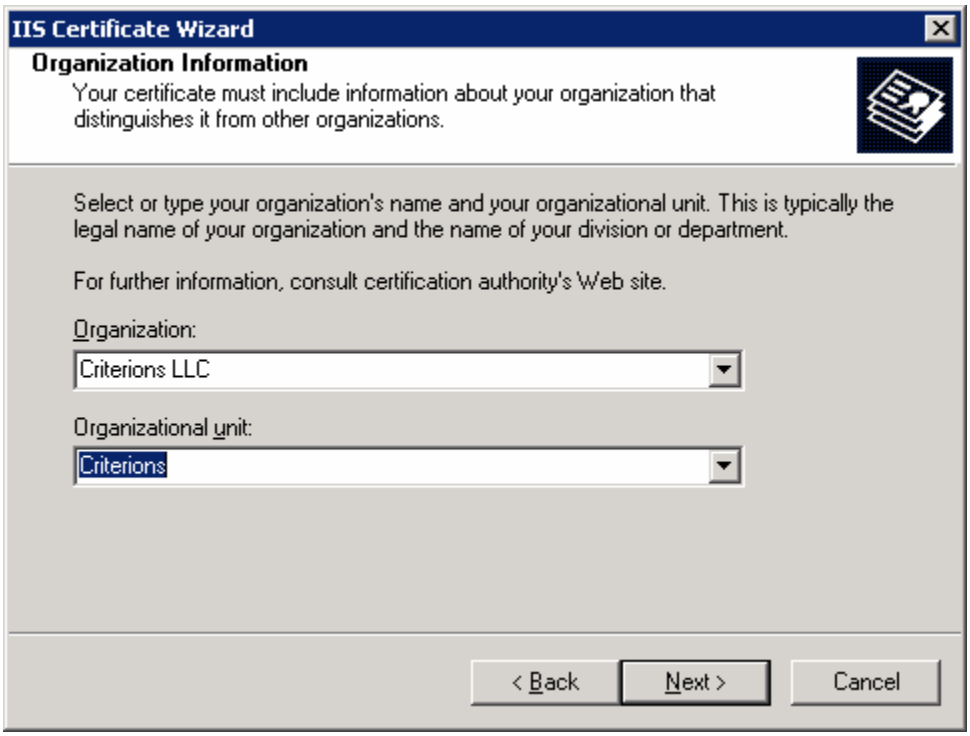
Select the first option, to 'Prepare the request now, but send it later'


IIS Certificate Wizard
Delayed or Immediate Request
You can prepare a request to be sent later, or you can send one immediately.
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?
Prepare the request now, but send it later
Send the request immediately to an online certification authority
< Back
Next >
Cancel

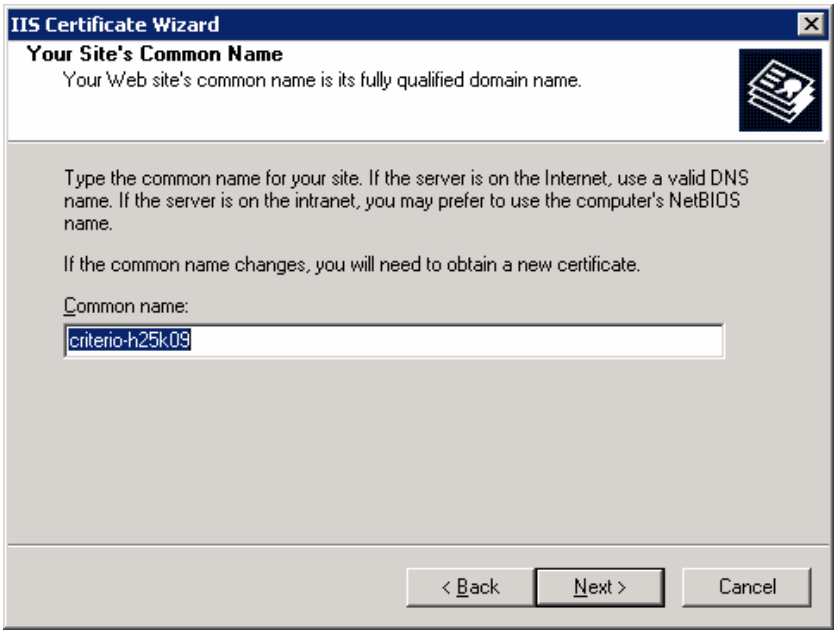
It's good practice to match the naming convention used in IIS, since we are working on the *Default Web Site* that is the name we will provide here. If your website is named differently in IIS, you may want to use that name. Leave the bit length at 1024 and leave the 'Select cryptographic service provider (CSP) for this certificate blank. Click next to advance.


IIS Certificate Wizard
Name and Security Settings
Your new certificate must have a name and a specific bit length.
Type a name for the new certificate. The name should be easy for you to refer to and remember.
Name:
Default Web Site
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.
Bit length:
1024
Select cryptographic service provider (CSP) for this certificate
< Back
Next >
Cancel

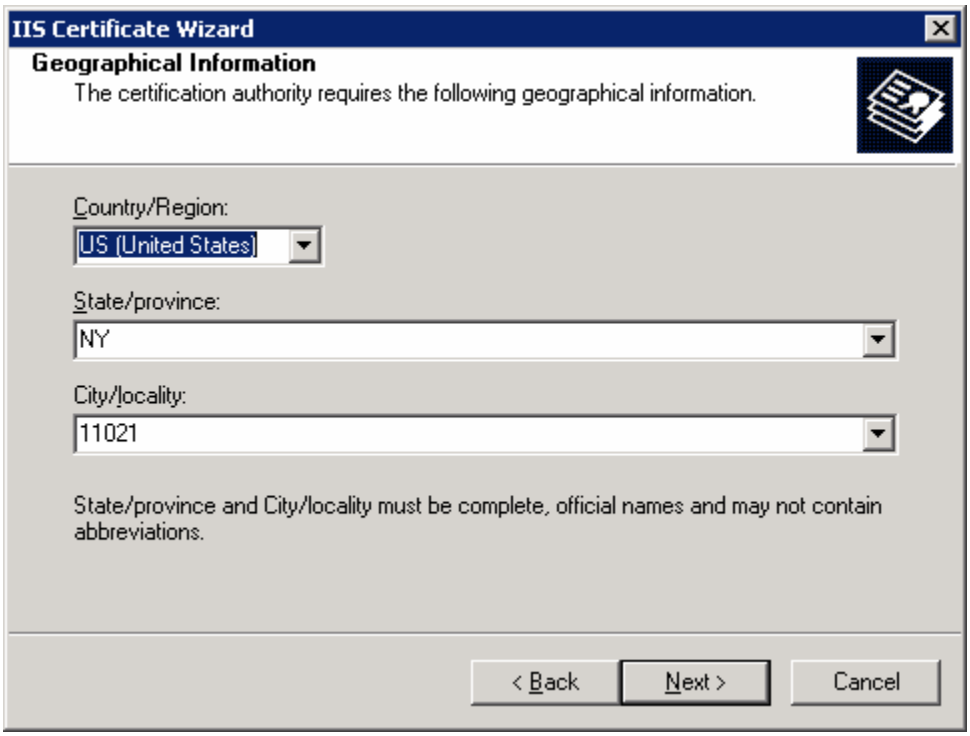
Provide the name of your Organization and Organizational Unit and click next to advance to the next form.


IIS Certificate Wizard
Organization Information
Your certificate must include information about your organization that distinguishes it from other organizations.
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.
For further information, consult certification authority's Web site.
Organization:
Criterions LLC
Organizational unit:
Criterions
< Back
Next >
Cancel

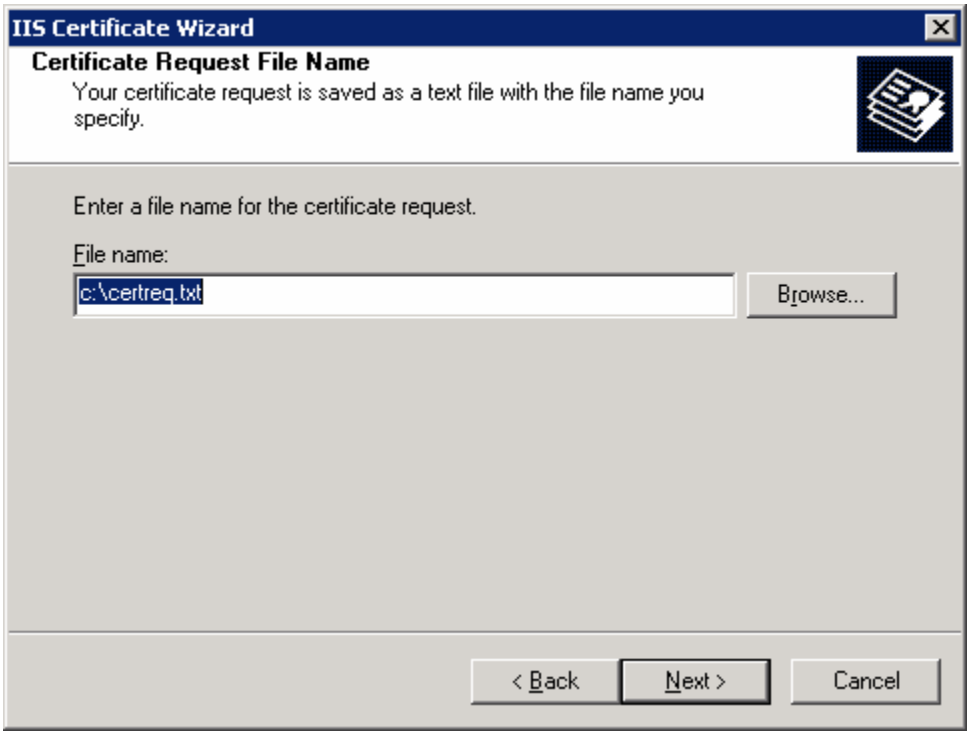
Next we have to provide either a DNS name (if you have purchased a DNS for your site from a 3rd party retailer such as GoDaddy.com) or the machine name of the server if the application will be hosted over the local intranet. Once entered click on next to advance to the next form.


IIS Certificate Wizard
Your Site's Common Name
Your Web site's common name is its fully qualified domain name.
Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.
If the common name changes, you will need to obtain a new certificate.
Common name:
criterio-h25k09
< Back
Next >
Cancel

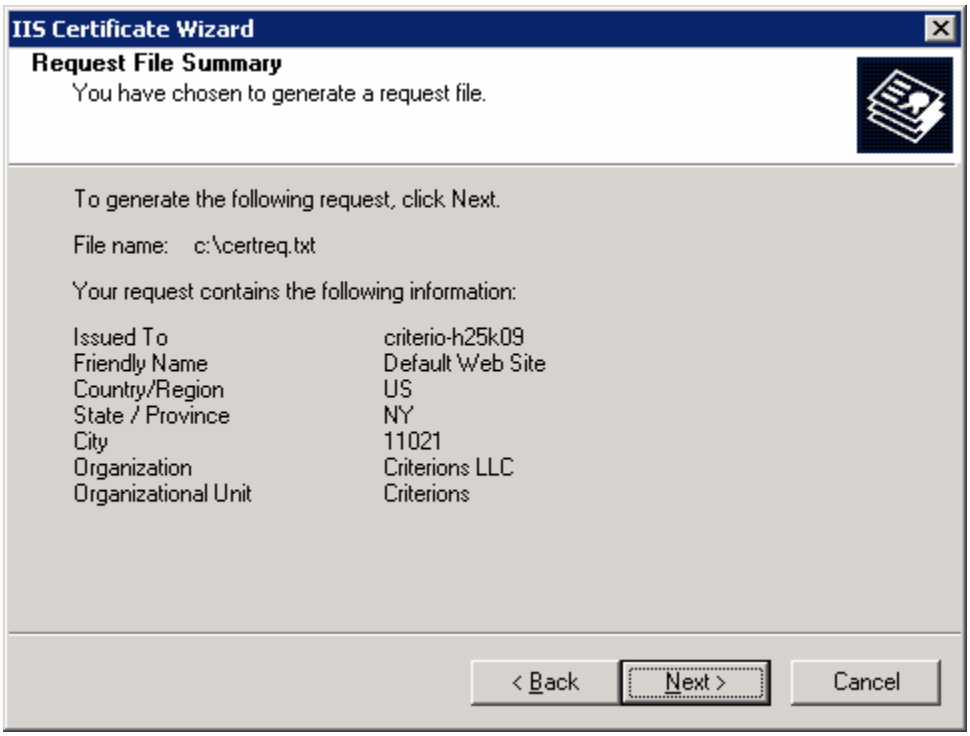
Next we provide the Country, State, and Zip Code the server will be residing in, then click 'Next'.



Last, we indicate where to save the certificate request.


IIS Certificate Wizard
Certificate Request File Name
Your certificate request is saved as a text file with the file name you specify.
Enter a file name for the certificate request.
File name:
c:\certreq.txt
Browse...
< Back
Next >
Cancel

We now verify that the information entered is correct, and click 'Next' to complete the certificate request.

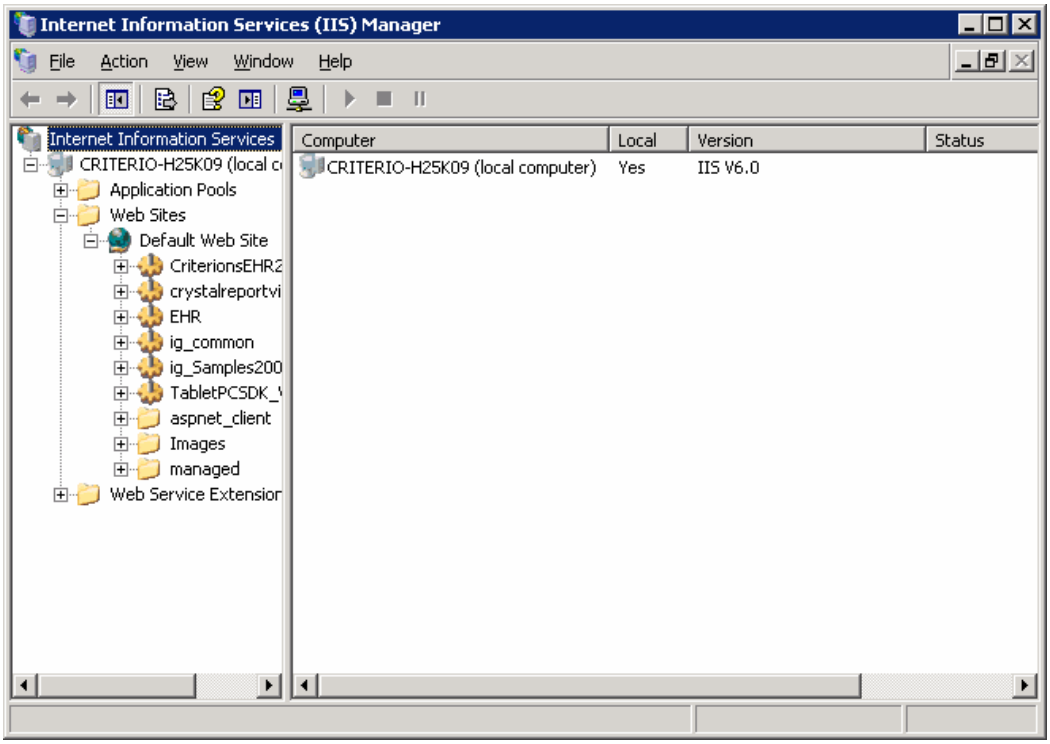


At this point, the user is to submit their certificate request to a valid 3rd party vendor such as GoDaddy.com. They may choose to do this on their own, or submit their certificate request to Criterions who will take care of the processing for them.

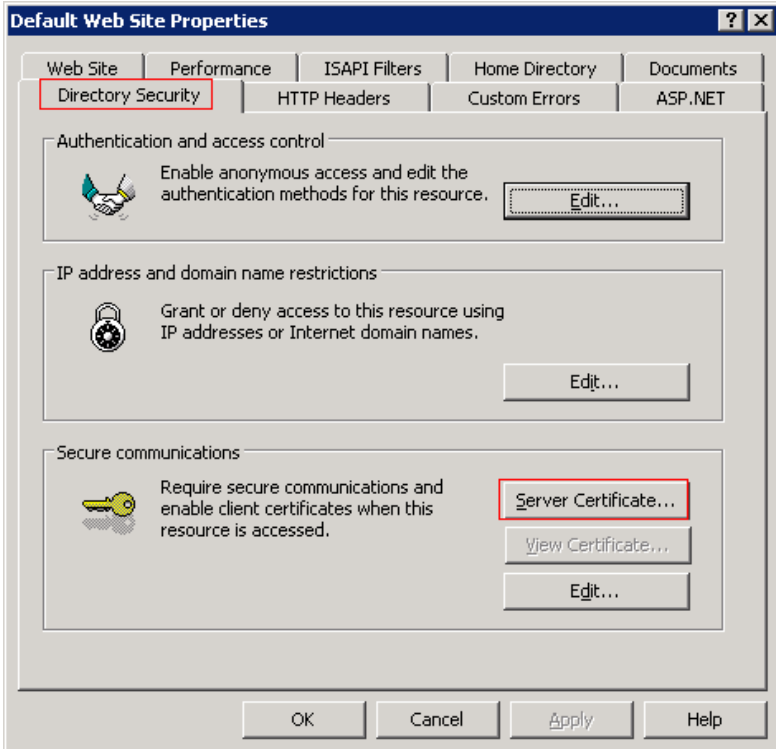
Part 2: Installing a Certificate

At this point you should have prepared your Certificate Request, submitted it to the proper party, and have been returned your certificate file (*.ctr).

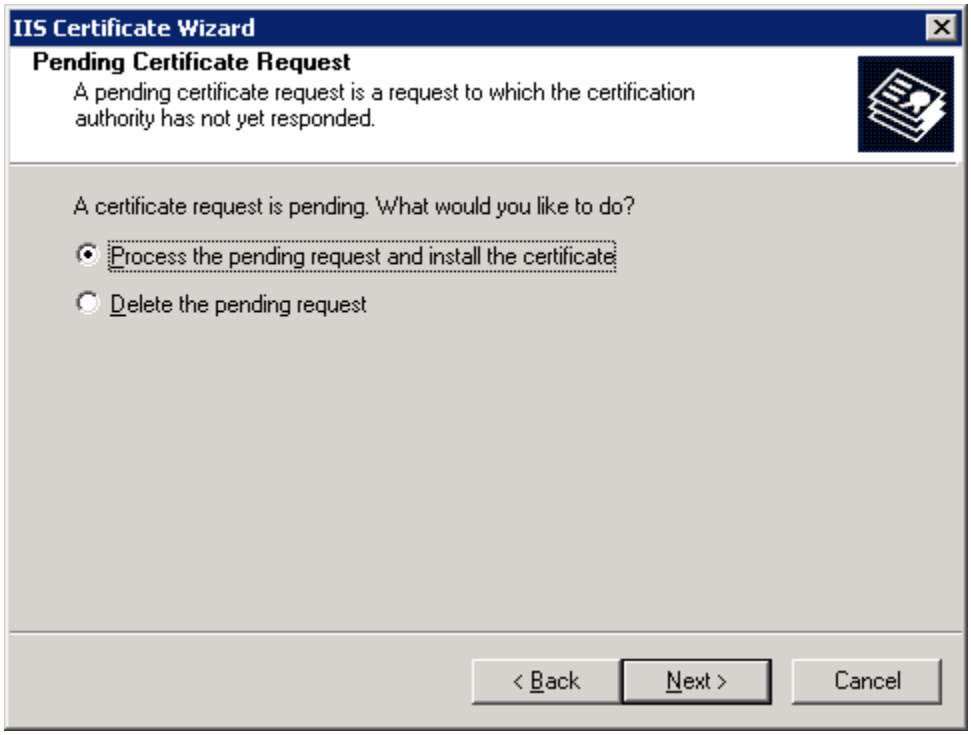
Open the *Internet Information Services (IIS) Manager* (found in the Administrative Tools portion of the Control Panel).



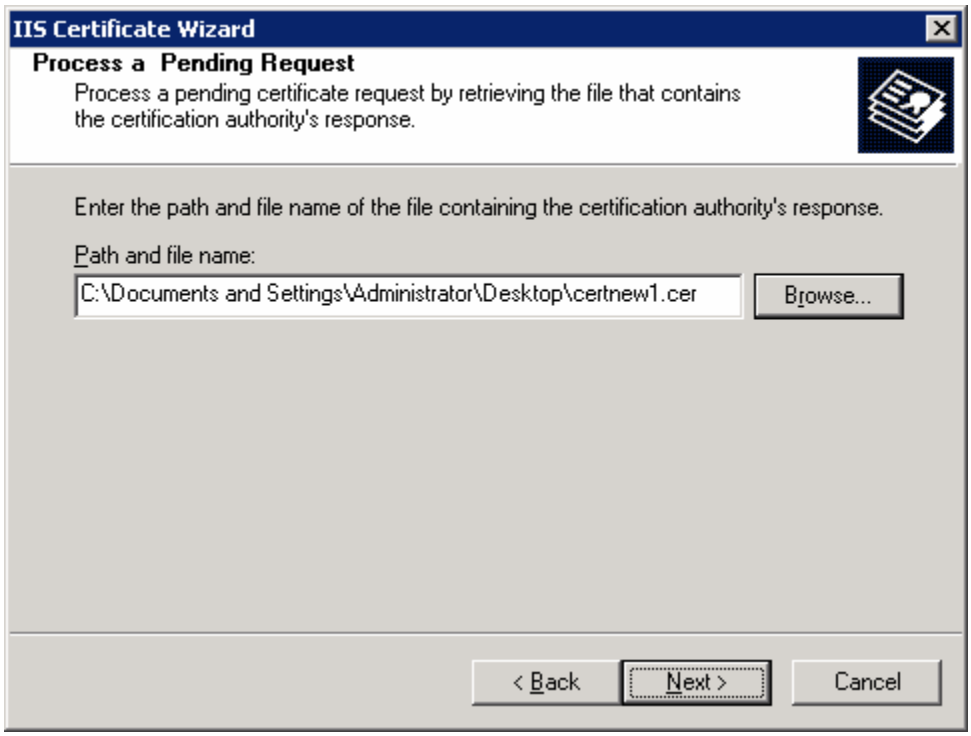
Select the Website you generated your certificate request for. Right click and select properties.



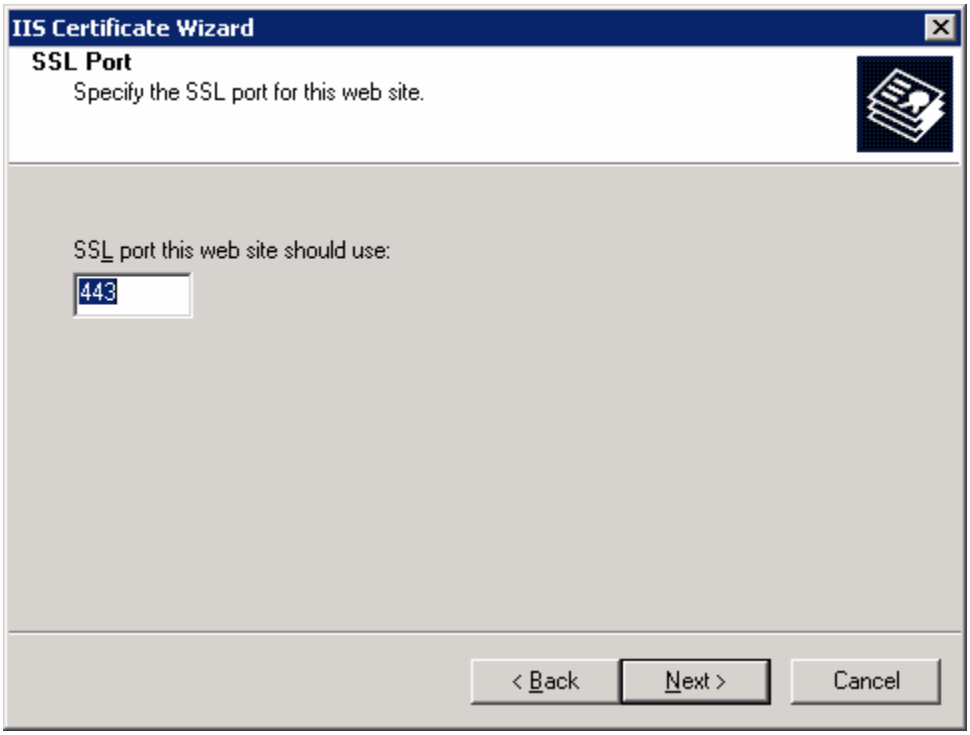
In the *Default Web Site Properties* window, select the 'Directory Security' tab and click on the 'Server Certificate' button to spawn the Web Server Certificate Wizard.


IIS Certificate Wizard
Pending Certificate Request
A pending certificate request is a request to which the certification authority has not yet responded.
A certificate request is pending. What would you like to do?
Process the pending request and install the certificate
Delete the pending request
< Back
Next >
Cancel

This time, we will be processing the certificate, so select the first option and click next.

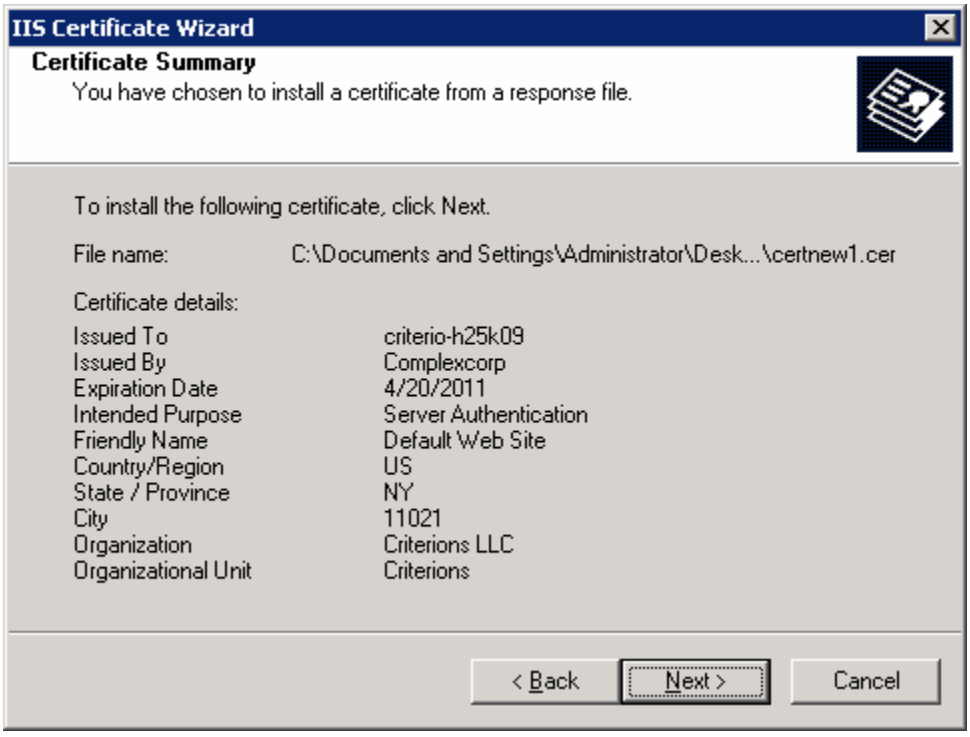

IIS Certificate Wizard
Process a Pending Request
Process a pending certificate request by retrieving the file that contains the certification authority's response.
Enter the path and file name of the file containing the certification authority's response.
Path and file name:
C:\Documents and Settings\Administrator\Desktop\certnew1.cer
Browse...
< Back
Next >
Cancel

We now use the browse button to locate the certificate (*.cer)file, and click on the next button.

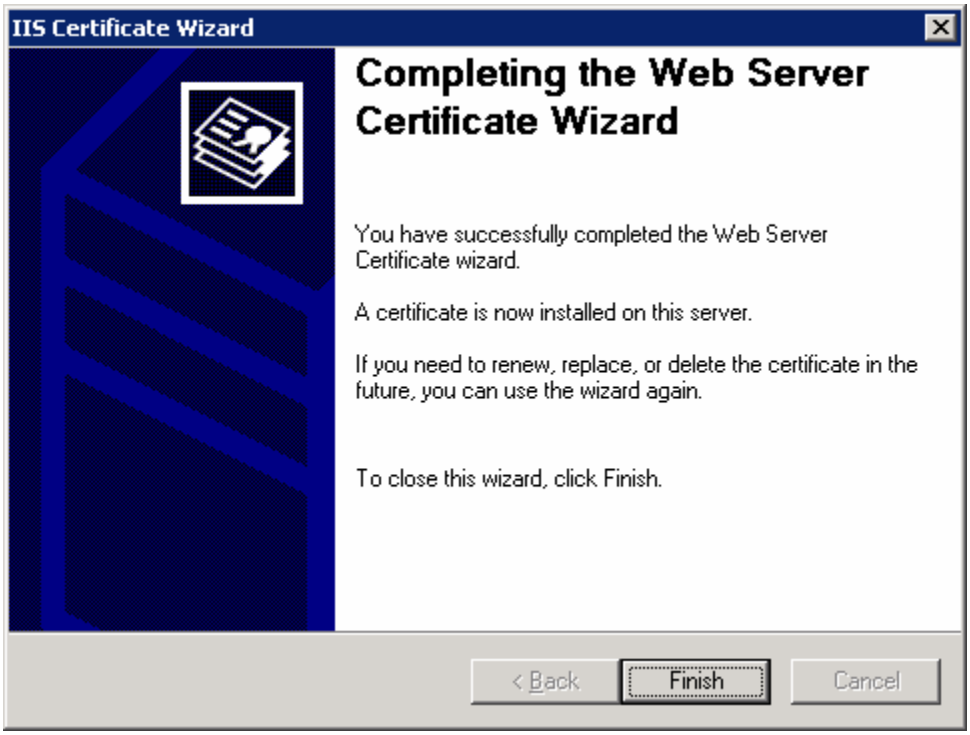


We are then prompted to dictate which port should be used for SSL. By default this port is 443, your network administrator may have it configured differently. If you are unsure of which port to use, consult with your network administrator, or check the properties on your router if you have access.

We are now prompted to review the properties tied to this certificate, by clicking the 'Next' button will officially install it.



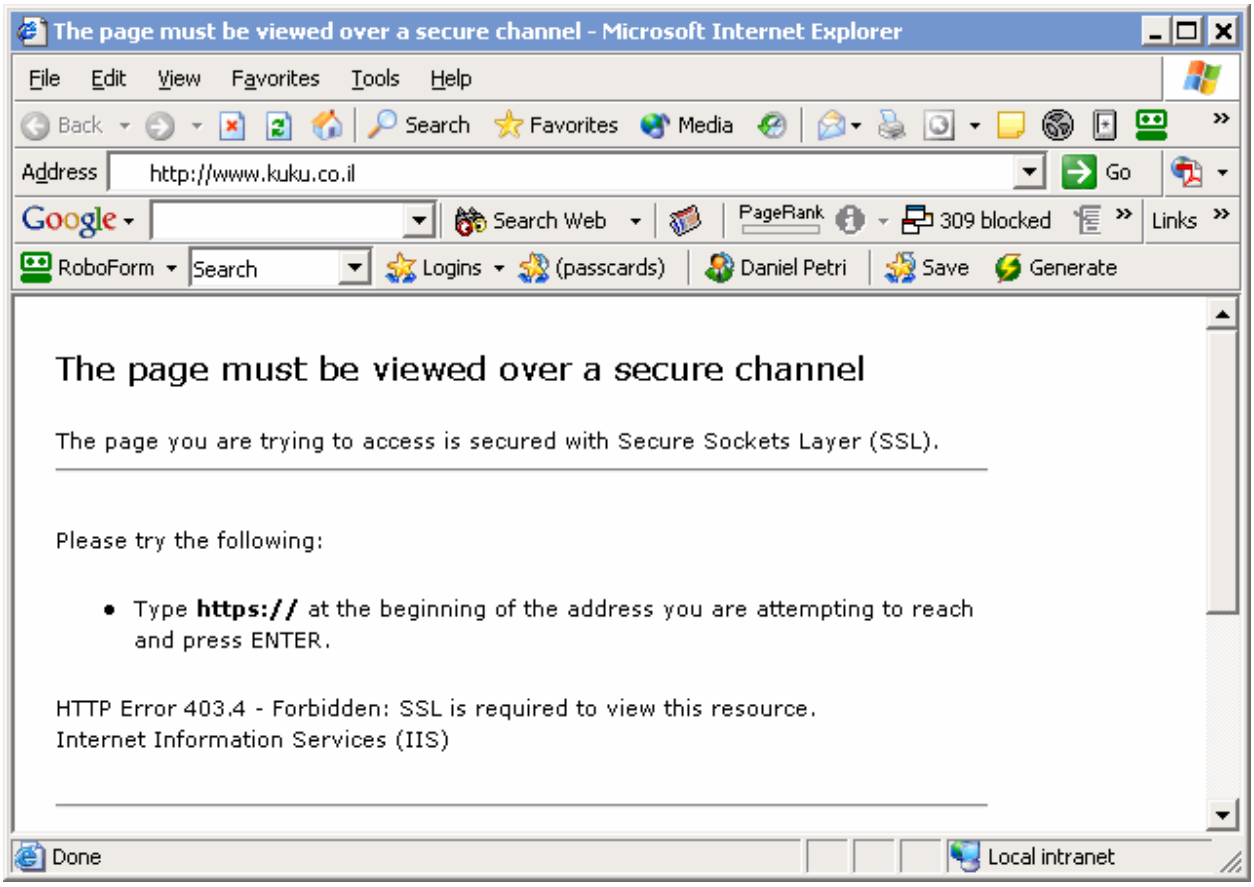
Click on the 'Finish' button in the next form, and the certificate installation is complete.


IIS Certificate Wizard
Completing the Web Server Certificate Wizard
You have successfully completed the Web Server Certificate wizard.
A certificate is now installed on this server.
If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.
To close this wizard, click Finish.
< Back
Finish
Cancel

Verify that SSL is working

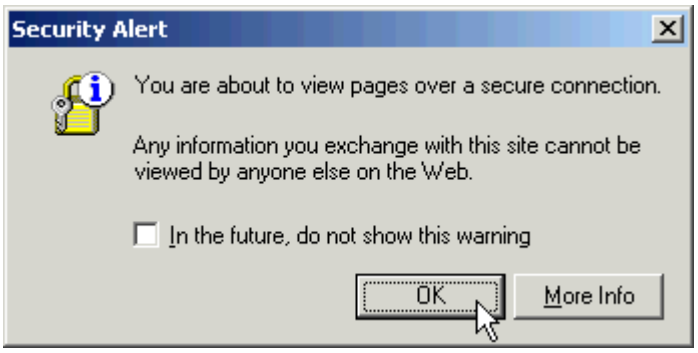
To test your new settings connect your open a browser and type your server's FQDN (or NetBIOS name, if on the LAN) in the address bar (for example: http://server200 for your Intranet, or http://www.kuku.co.il for the Internet).

Since you still used HTTP (plain text http, using TCP port 80) you'll get the following error message:


The page must be viewed over a secure channel - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.kuku.co.il
Go
Google
Search Web
PageRank
309 blocked
Links
RoboForm Search
Logins (passcards)
Daniel Petri
Save
Generate
The page must be viewed over a secure channel
The page you are trying to access is secured with Secure Sockets Layer (SSL).
Please try the following:
Type https:// at the beginning of the address you are attempting to reach and press ENTER.
HTTP Error 403.4 - Forbidden: SSL is required to view this resource.
Internet Information Services (IIS)
Done
Local intranet

Now re-type the URL by using HTTPS instead of HTTP. You should be able to view your website.

You'll receive a Security Alert window. Click Ok.


Security Alert
You are about to view pages over a secure connection.
Any information you exchange with this site cannot be viewed by anyone else on the Web.
In the future, do not show this warning
OK
More Info

If configured correctly, you should be able to connect to your now SSL-protected website.

To verify that you're using SSL try to find a small yellow lock icon on the browser lower right corner . Double click the lock icon.

A Certificate window will open. Review the information that is entered into the certificate and click Ok.

Note: Make sure you renew your certificate a few weeks before it expires in order to prevent mishaps like this one: Expired SSL Website Certificate.

4.0 - Password Transfer

All password transfer is handled using System.Security.Cryptography.

The System.Security.Cryptography namespace provides cryptographic services, including secure encoding and decoding of data, as well as many other operations, such as hashing, random number generation, and message authentication.

For additional information please visit:

http://msdn.microsoft.com/en-us/library/system.security.cryptography(vs.71).aspx

http://www.faqs.org/rfcs/rfc1321.html

5.0 – Power Supply

Note: Client System Administrators should be authority regarding all hardware setup.

Clients are advised to have power redundancy to prevent data loss in the even of power failure.

Uninterrupted Power Supplies (UPS) should be provided at every station.

6.0 – Network/System Requirements

	Clients are responsible for the installation and upkeep of items related to hardware/malware prevention. We strongly recommend the use of proven Malware/Antivirus protection programs (such as Symantec Anti-Virus, McAfee Anti-Virus) on all server and client stations and schedule automated scans to run regularly.

	To Properly run all functionality of the EHR each PC must have the following installed. Tablet SDK: http://www.microsoft.com/downloads/details.aspx?familyid=B46D4B83-A821-40BC-AA85-C9EE3D6E9699&displaylang=en .Net 2.0: http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en Ajax 1.0: http://www.microsoft.com/downloads/details.aspx?FamilyID=ca9d90fa-e8c9-42e3-aa19-08e2c027f5d6&displaylang=en Adobe Reader: http://download.cnet.com/Adobe-Acrobat-Reader/3000-2378_4-10349804.html

Performance and security of Criterions products, as with any IT system, is contingent on many parts working effectively together. Below is a list of Benchmark settings and minimum requirements.

Benchmark Performance: Using Windows 2008 on an Quad Core processor with 4Gb of RAM and 500Gb RAID 5 drive, on a HL switch with 20 ports, with 20 concurrent users, entering data, running the EHR and Practice management, running reports, most queries return back within 4 seconds.

The system also has a number of minimum requirements that should be met.

6.1 - Client is required to get a high speed internet connection from a reputable ISP

6.2 - Must have a router or hub with enough connectivity to handle the desired number of connections.
-router may include firewall
-client may use windows firewall for added security

6.3 - **Minimum hardware requirements for IIS and Oracle.**

6.3.1 - For IIS Server:

FOR WINDOWS 2003

- **For an x86-based computer**:

  - One or more processors with a recommended minimum speed of 550 megahertz (MHz). The minimum supported speed is 133 MHz. A maximum of eight processors per computer is supported. Processors from the Intel Pentium/Celeron family, AMD K6/Athlon/Duron family, or compatible processors are recommended.
  - 256 megabytes (MB) of RAM (recommended minimum). 128 MB is the minimum supported, and 32 gigabytes (GB) is the maximum supported.
    For computers with more than 4 GB of RAM, be sure to confirm hardware compatibility by clicking the appropriate link in Support resources.

- **For an Itanium-based computer**:

  - One or more processors with a minimum speed of 733 MHz. A maximum of eight processors per computer is supported.
  - 1 GB of RAM minimum, 1024 GB (1 Terabyte) maximum.
    For computers with more than 4 GB of RAM, be sure to confirm hardware compatibility by clicking the appropriate link in Support resources.

- **For an x64-based computer**:

  - One or more processors with a minimum speed of 1.4 GHz. A maximum of eight processors per computer is supported.
  - 1 GB of RAM minimum, 1024 GB (1 Terabyte) maximum.
    For computers with more than 4 GB of RAM, be sure to confirm hardware compatibility by clicking the appropriate link in Support resources.

  - A hard disk partition or volume with enough free space to accommodate the setup process. To ensure that you have flexibility in your later use of the operating system, we recommend that you allow considerably more space than the minimum required for running Setup, which is approximately 2 GB to 3 GB for x86-based versions of Windows Server 2003, and 4 GB for Itanium-based and x64-based versions of Windows Server 2003. The larger amount of space is required if you are running

Setup across a network instead of from a CD-ROM, or if you are installing on a FAT or FAT32 partition in the case of x86-based or x64-based versions of Windows Server 2003. (NTFS is the recommended file system for both x86-based and x64-based versions of Windows Server 2003. Itanium-based versions of Windows Server 2003 support only NTFS).
In addition, a domain controller upgrade from Windows NT 4.0 could require much more space than other upgrades or installations, because the existing user accounts database can expand by as much as a factor of ten during the upgrade, as Active Directory functionality is added.

6.3.2 - FOR ORACLE 10G Database on a Windows Based Machine

Oracle 10g PC Minimum Hardware Requirements:

Physical memory (RAM)	512 MB minimmum
Virtual memory	Double the amount of RAM
Temp disk space	Hard disk space 1.5 GB
Video adapter	256 colors
CPU Processor	200 MHz minimum

Oracle 10g Minimum Windows System Requirements:

Architecture	32 bit or 64 bit
Windows OS	- Windows NT Server 4.0 - Windows NT Server Enterprise Ed. 4.0 - Windows NTTerminal Server Edition with SP 6 - Windows 2000 with SP 1 or higher - Windows Server 2003 - Windows XP Professional
Network protocol	- TCP/IP - TCP/IP with SSL - Named Pipes

	Minimum Requirements are given only as a guideline by Criterions. System Administrators are responsible for determining client needs and required hardware/software to accomplish those needs. For more information, please contact 516.466.1942 or info@criterions.com

7.0 – HL7 – Electronic Lab Retrieval

HL7, or Health Language 7, is one of several American National Standards Institute (ANSI) -accredited Standards Developing Organizations (SDOs) operating in the healthcare arena. Most SDOs produce standards (sometimes called specifications or protocols) for a particular healthcare domain such as pharmacy, medical devices, imaging or insurance (claims processing) transactions. Health Level Seven's domain is clinical and administrative data.

With your Criterions products you can receive lab results from major labs electronically that automatically populate a patient's documents.

With Criterions products, we do not 'pull' documents from the labs themselves or any other external source.

To receive labs, practices must contact their labs to have the labs run their own local applications, per their specifications, to bring data into client local site. Criterions products will access information from the internal lab source.

	Installation of lab systems and the security protocols associated with accessing outside information is the sole responsibility of the practice and their system administrators.

8.0 – Electronic Billing

Electronic Billing is transmitted using the standards implemented by the carrier in question, or via a clearing house. If you choose to bill electronically, Criterions uses Emdeon for electronic billing.

Emdeon provides a secured web service that is integrated into the Criterions billing system. Security is in compliance with Emdeon standars (see Emdeon_ITS_User_Guide_20081021x[1].pdf).

	Installation of lab systems and the security protocols associated with accessing outside information is the sole responsibility of the practice and their system administrators.

9.0 – Peripherals – Printing, Scanning, Faxing, Email

The networking of Printers, Scanners and other devices is the responsibility of the practice.

Printers and Scanner – Criterions only supports locally installed scanners (1 per station). Printers can be local or shared. Shared printers are installed on IIS server on a per-location basis using standard TCP/IP ports.

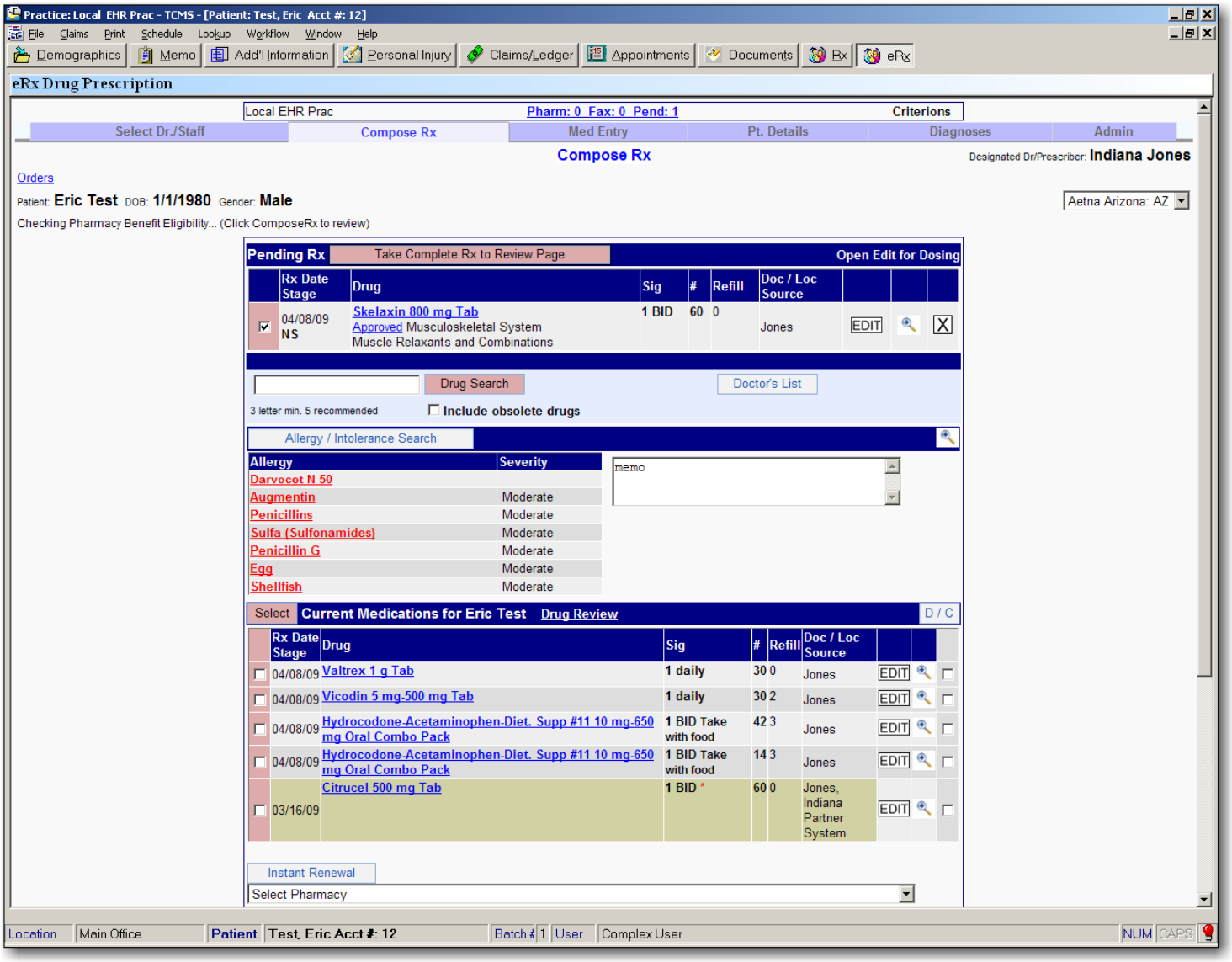
Upon login to the system the user indicates whether or not they are currently inside the office, or working from a remote location. If they are inside the office, all printed reports are fed to a queue, which is managed by the application server, which will print to any designated device on their network. If they are outside the office, they may choose to print to devices local to their current location. There is no way to input information into the system directly through peripheral devices.

Clients may choose to purchase one of the following fax solutions for transmission of documents via fax; EasyLink or Castelle Fax Server.

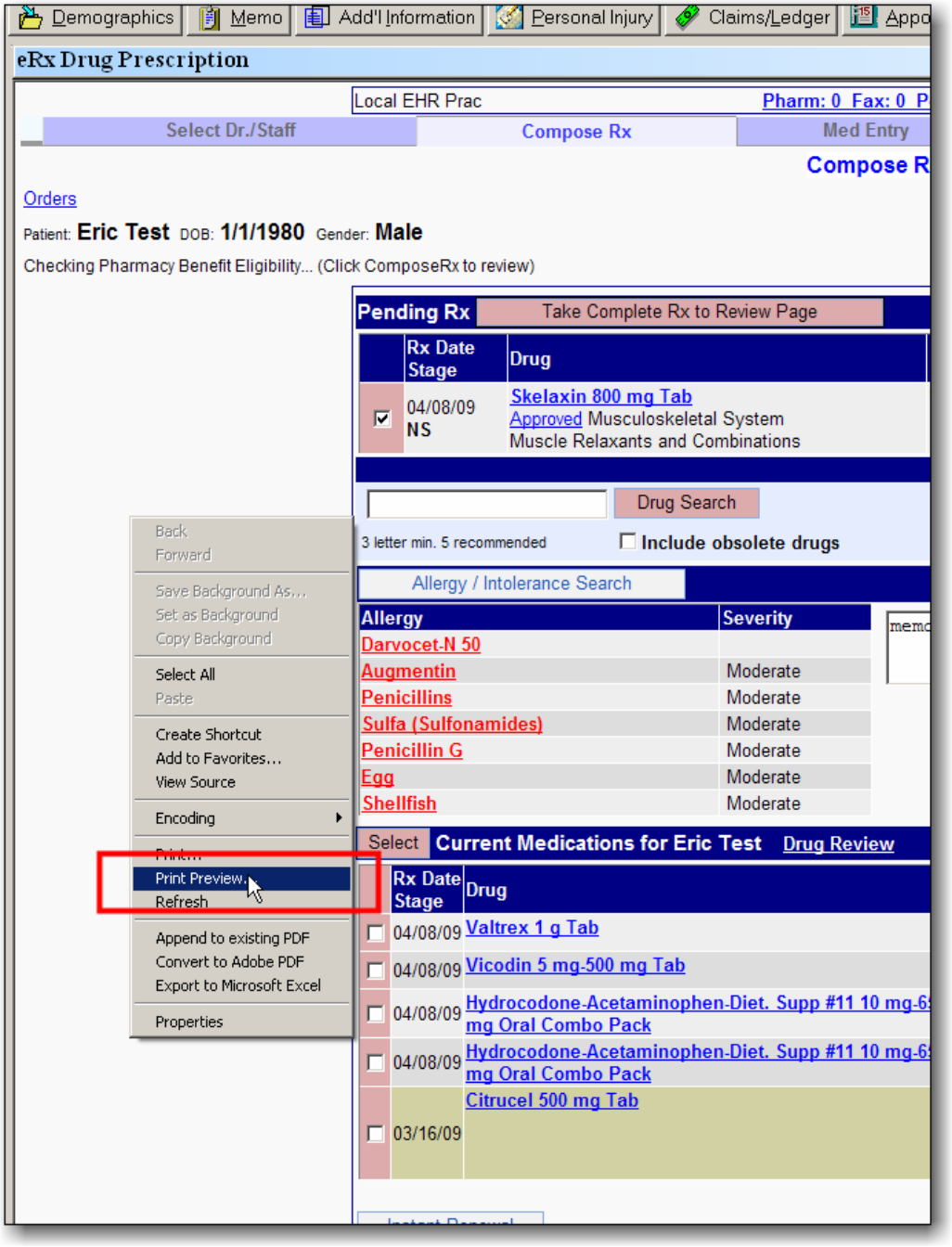
Criterions EHR includes it own proprietary secure messaging system. This is for internal messaging only and does not connect to any mail server or outside systems. They system will neither accept nor send email to addresses outside of the practice's EHR.

Setting Up eRx Printing Alignment

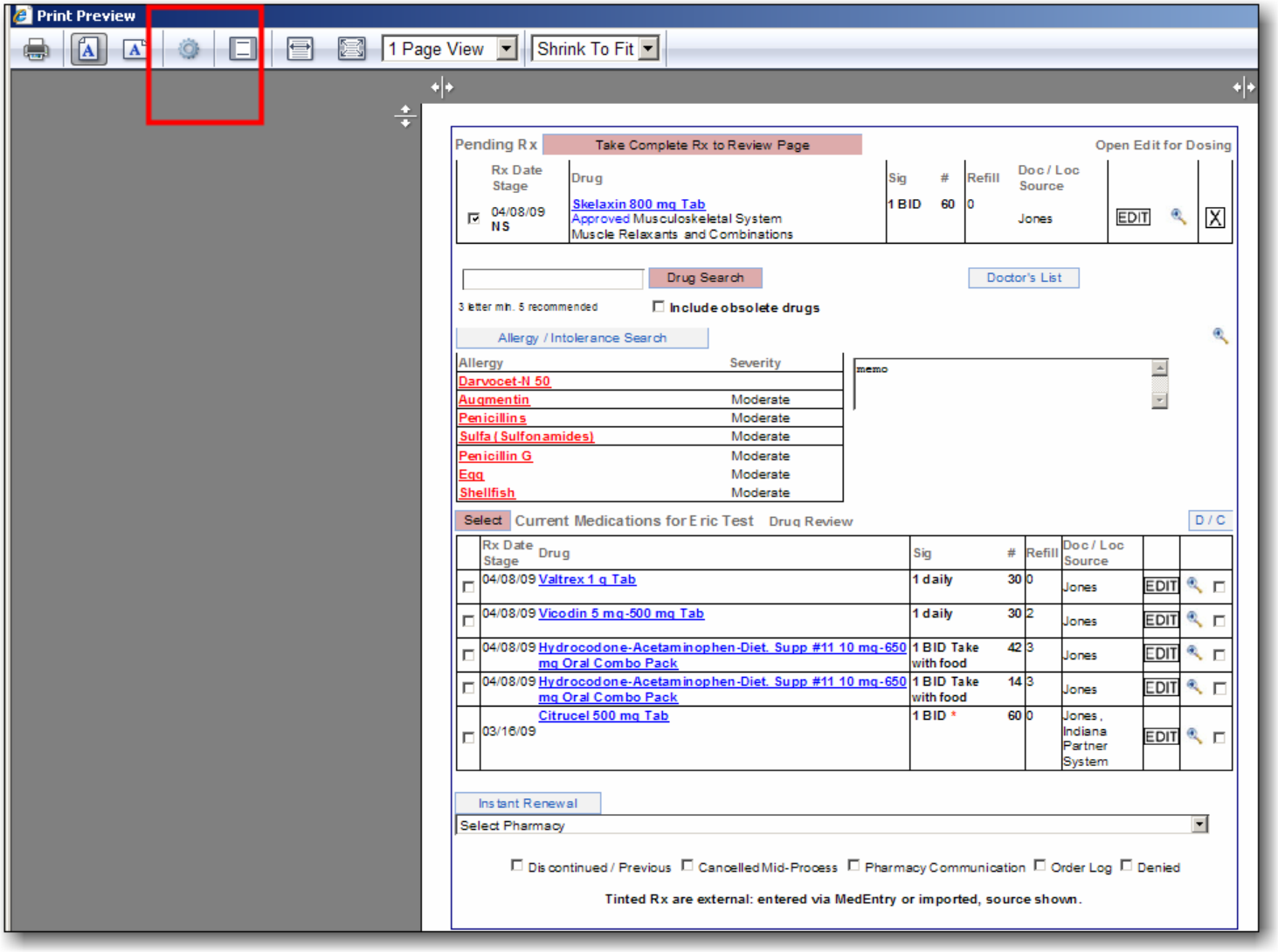
Because eRx goes through internet explorer each computer must have its IE printer settings customized.



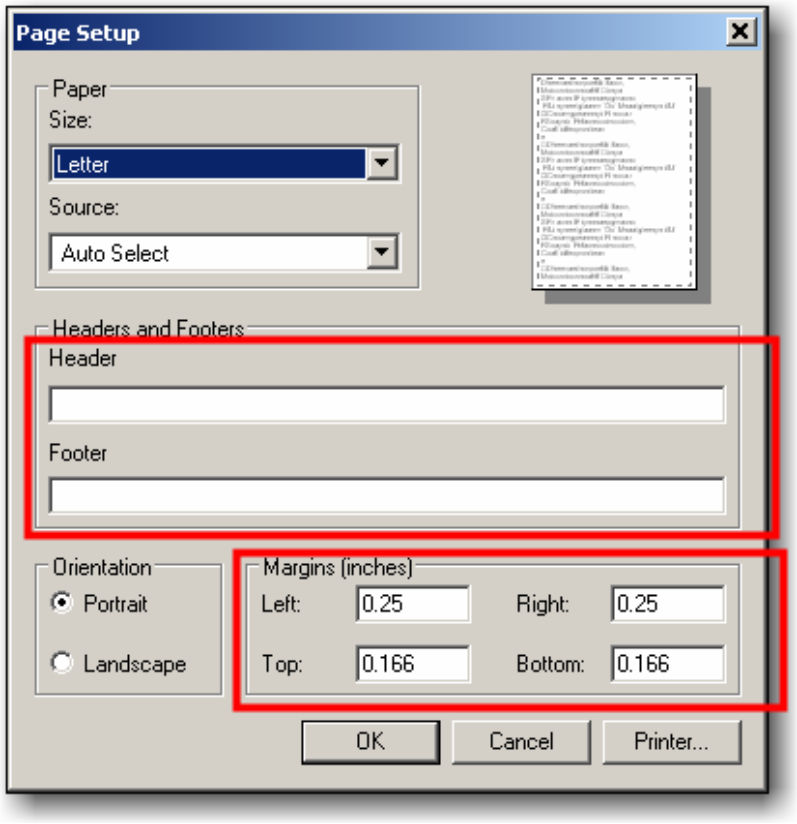
Right Click on the internet explorer page.



Select Print Preview.



Select the Preferences icon.



Make sure that the "Header" and "Footer" are blank.

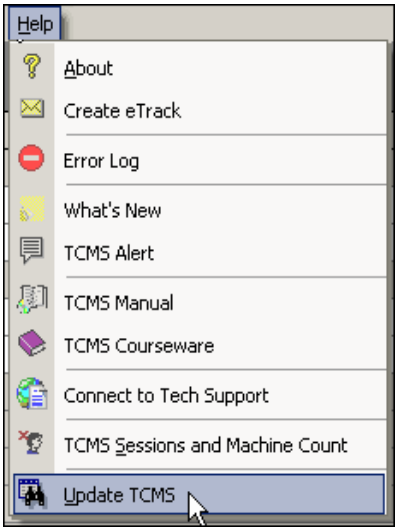
Make sure Margins are set to the above settings.

10.0 – Updates to System

TCMS

To update TCMS first access the "What's New" icon to learn about the updates and requirements for a TCMS update.

Next, Click **Help-> Update TCMS**.



If you are currently on the latest version of TCMS the following error will appear:

If an update is available,

EHR

	Due to the potentially impact of an EHR upgrade on client operations, all EHR upgrades are managed by Criterions Implementation Specialists. Specialists are charged with determining impact, downtime (if applicable), scheduling, and notification to system administrators. Account Specialists are tasked with clearly conveying to clients to changes to system and processes, as well as any client requirements that may need to be met.

	The Criterions EHR has no Operating System (OS) prerequisites for patch installation. Clients are encouraged to maintain OS self-patches and all client systems should be set to Windows Auto Update to maintain currency of their systems.

To view available updates to your system, please visit www.criterions.com and use your client ID and password to login to the client website using the "login" link. Once you have determined that the patch is applicable to your operations and you would like to proceed, the following steps need to be taken.

1. Client contacts Criterions Account Specialist to request patch update.
2. Criterions Implementation Specialist will be assigned to your account.
3. Implementation Specialist determines patches to apply, impacted aspects of client system and required client steps to be taken (e.g. TCMS update, estimated downtime, user access, etc).

	While in most cases updates to the Criterions EHR will not result in any change of performance or usage of TCMS Practice Management, there are occasions where users will be required to exit both systems to complete a patch. In some cases, practices will be required to update their TCMS system prior to Criterions EHR updates. In these cases, please refer to the above TCMS update section for instructions on how to update your TCMS.

4. Account specialist is informed of the changes and the impact to the client.
5. Account specialist reviews impact with client and relays pertinent information

    a: Instruction manual excerpts given as necessary

    b: Client processes are reviewed as necessary

    c: Web-Demo or Live Instruction given as necessary

    d: System Administrator is informed of update information pertaining to client system
6. Patch Request Form is completed.
7. Patch update is scheduled.
8. Patch is performed at scheduled time.
9. Patch test script is executed by Criterions Implementation Specialist.
10. Client System Administrator is notified of patch completion.

11. Client contact is notified by Account Specialist of patch installation and additional steps, if any, required for use of updated system.
12. Training via web or in-person is delivered, if necessary.
13. Patch release is closed.

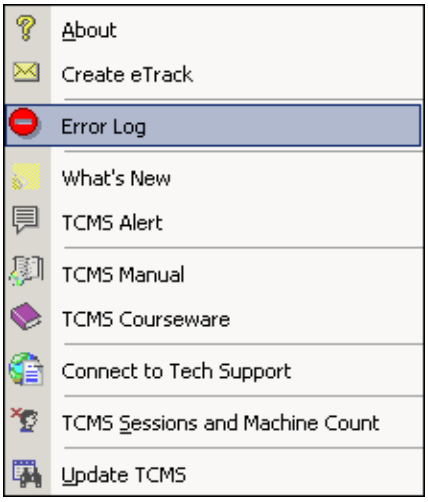
To contact your Account Supervisor, please call 516.466.1942 or email us at info@criterions.com.

	Should any changes be made to the patch process, all clients will be informed by their Account Supervisor with updated protocols.

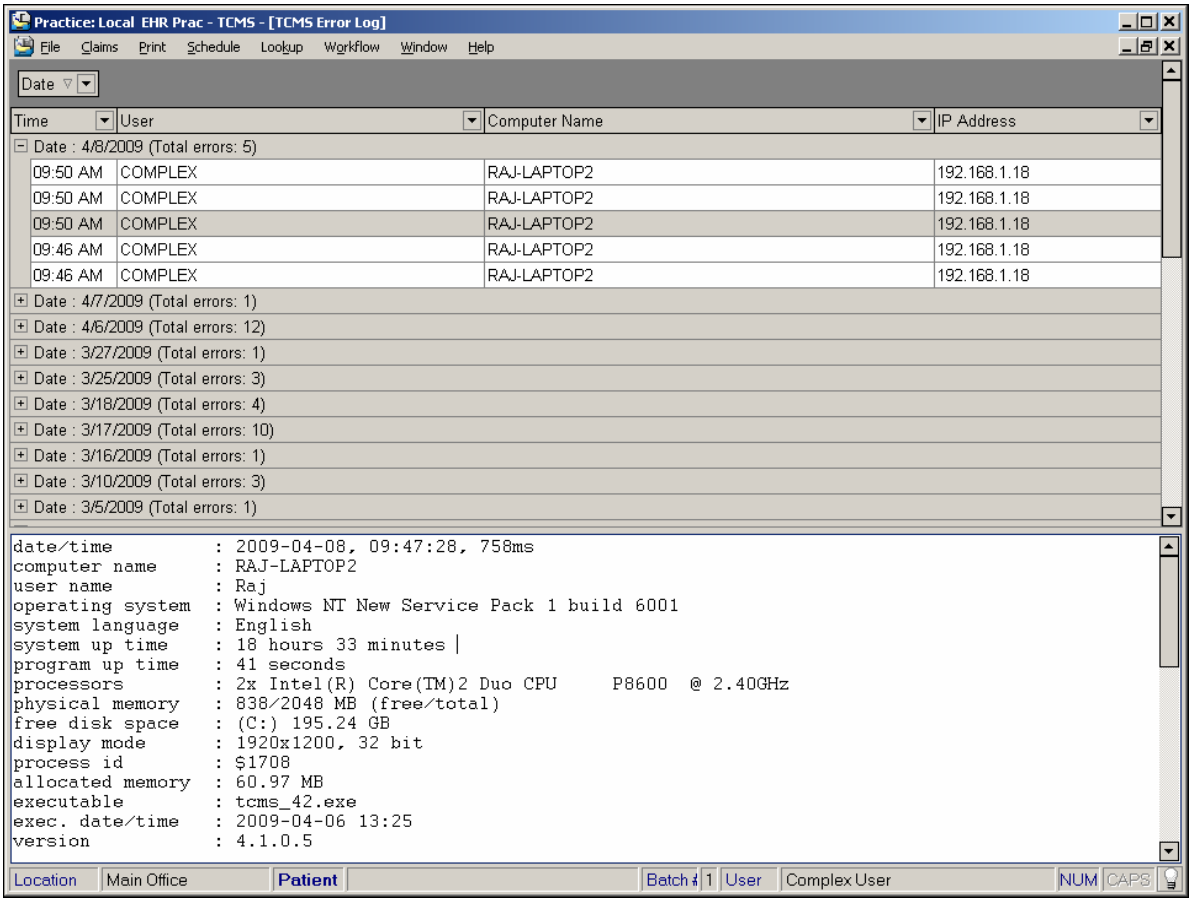
11.0 – Error Logs

Through most of the Criterions systems errors are answered with a pop-up box that will give instructions regarding the steps required to

Should you experience system errors, Criterions products record these errors in an Error Log located in TCMS under **HELP -> ERROR LOG**.



The Error Log will display.


Practice: Local EHR Prac - TCMS - [TCMS Error Log]
File Claims Print Schedule Lookup Workflow Window Help
Date
Time User Computer Name IP Address
Date : 4/8/2009 (Total errors: 5)
09:50 AM COMPLEX RAJ-LAPTOP2 192.168.1.18
09:50 AM COMPLEX RAJ-LAPTOP2 192.168.1.18
09:50 AM COMPLEX RAJ-LAPTOP2 192.168.1.18
09:46 AM COMPLEX RAJ-LAPTOP2 192.168.1.18
09:46 AM COMPLEX RAJ-LAPTOP2 192.168.1.18
Date : 4/7/2009 (Total errors: 1)
Date : 4/6/2009 (Total errors: 12)
Date : 3/27/2009 (Total errors: 1)
Date : 3/25/2009 (Total errors: 3)
Date : 3/18/2009 (Total errors: 4)
Date : 3/17/2009 (Total errors: 10)
Date : 3/16/2009 (Total errors: 1)
Date : 3/10/2009 (Total errors: 3)
Date : 3/5/2009 (Total errors: 1)
date/time : 2009-04-08, 09:47:28, 758ms
computer name : RAJ-LAPTOP2
user name : Raj
operating system : Windows NT New Service Pack 1 build 6001
system language : English
system up time : 18 hours 33 minutes
program up time : 41 seconds
processors : 2x Intel(R) Core(TM)2 Duo CPU P8600 @ 2.40GHz
physical memory : 838/2048 MB (free/total)
free disk space : (C:) 195.24 GB
display mode : 1920x1200, 32 bit
process id : $1708
allocated memory : 60.97 MB
executable : tcms_42.exe
exec. date/time : 2009-04-06 13:25
version : 4.1.0.5
Location Main Office Patient Batch # 1 User Complex User NUM CAPS

We document errors in a log accessible to the System Administrator from the application's virtual directory. The Oracle error descriptions and error codes are listed in it, as well as internal error codes. For a complete listing of Oracle error code go to http://ora-code.com/ or http://www.oracle.com/pls/db92/db92.error_search.

This information is used by Criterions developers to pinpoint application failures and provide resolutions.

The Error Log records the date, time, workstation, workstation information, and error information. Using this information, System Admins or Criterions staff can troubleshoot the problem.

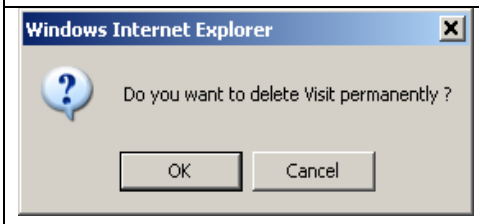
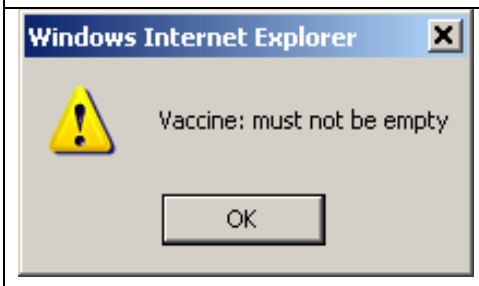
Common System Error Messages

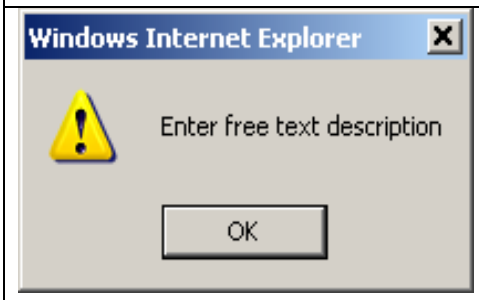
Exception Message :	Code	Meaning	Resolution
" " is not a valid integer value.		A null value was entered in a field that requires an integer.	Ensure all required fields have the required integer and save again
connection lost contactProcess ID: 5216Session ID: 1627 Serial number:	ORA-03135:	Connection to the server was lost.	Reinitiate session.

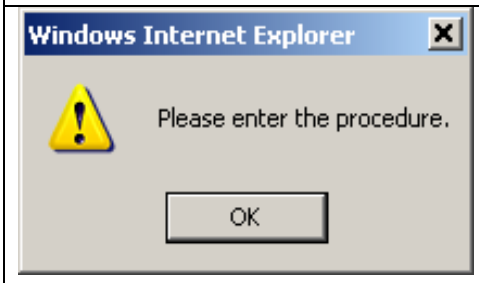
Exception Message :	Code	Meaning	Resolution
37278.			
You cannot access field data beyond Eof.		The query that was submitted has completed without finding any results.	Check what was sought and resubmit query.
List index out of bounds (-1).		The query that was submitted is looking for a value that is out of range.	Check query and submit again.
unique constraint (<<FIELDNAME>>) violated.	ORA-00001:	When entering a value into a Field, a user entered a code that already exists.	The system requires certain fields to be unique. Check the value is unique and reenter.
not connected to ORACLE.	ORA-03114:	There is no connection to the oracle server.	Establish a connection to the server.
Error in File :Print job busyConnect.Retrieve <PEGetNTables>.	Error:524	The print job could not be run.	Attempt print again. If error remains, logout of system
Not enough storage is available to process this command..		The computer has run out of memory.	Close other applications and attempt process again.
Field '<<FIELDNAME>>' must have a value.		The field in the <<FIELDNAME>> section must have a value before saving.	Enter value, attempt save again.
check constraint (TCMS_DATA.CK_ALLOWED) violated	ORA-02290:	The values being inserted do not satisfy the named check constraint.	Do not insert values that violate the constraint.
cannot insert NULL into ("TCMS_DATA"."USERLOGIN"."USERID")	ORA-01400:	The field requires a value.	Enter a valid value. Run process again.

Navigation Errors

User errors generate warning or error messages for the user to view with the required solution to resolve the conflict. They are stated in plain English and are pertinent to the screen the user is viewing. Error messages and warnings must have an acknowledgement by the user prior to any additional steps being taken. This acknowledgement is either a single option click to close the error message or a dual option choice that will direct additional actions. Some examples are listed below.

User Errors and Warnings	Location	Resolution
	Phone Encounter	User must select a diagnosis before entering a new Rx.
	Removing a visit will prompt a user to confirm the operation.	
	Vaccine	Complete the "Dose" field prior to saving
	Vaccine	Complete the "Vaccine" field prior to saving
	Vaccine	Complete the "Done by" field prior to saving.

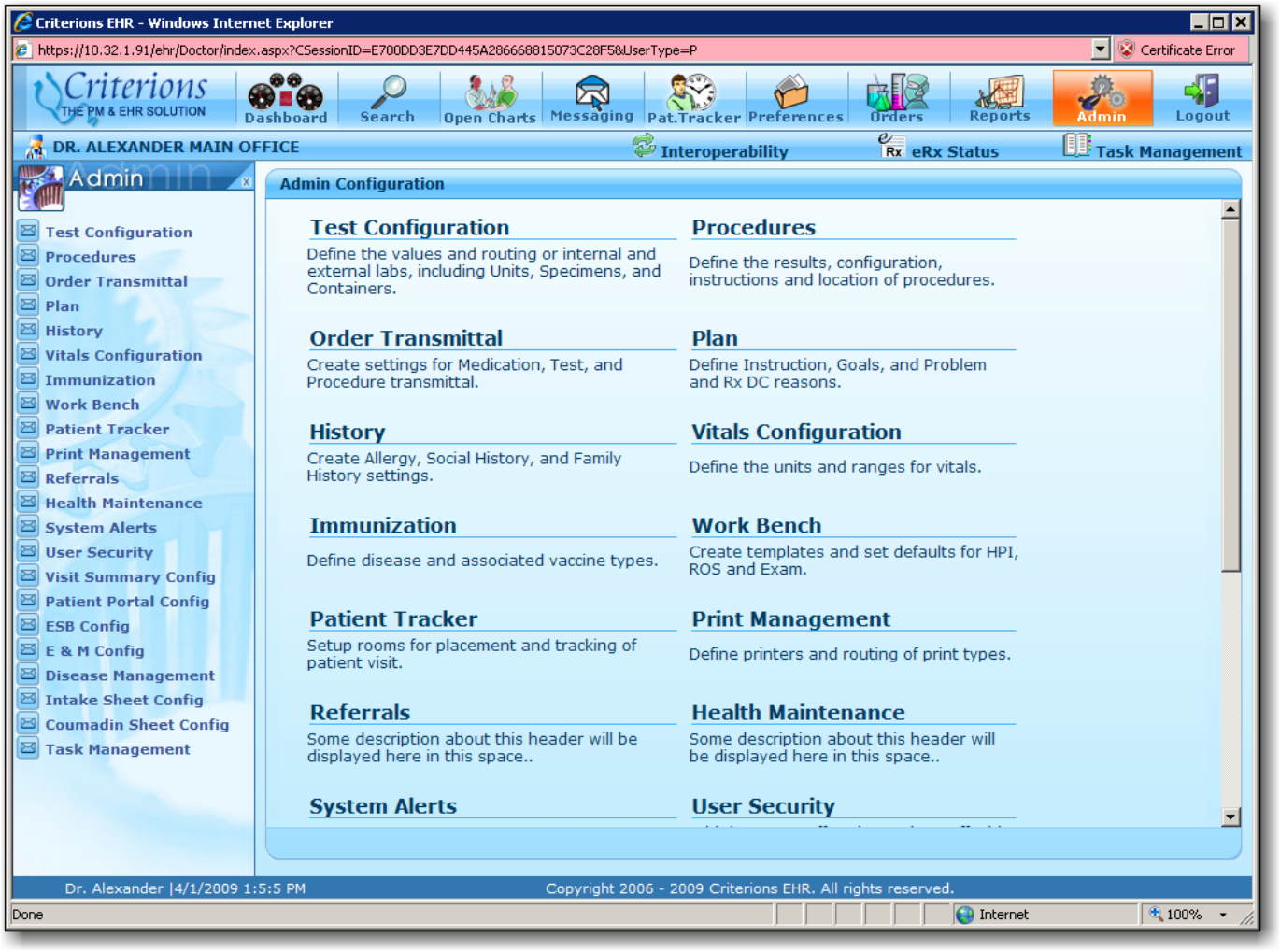
User Errors and Warnings	Location	Resolution
	Advanced Directives	Complete the First Name field.
	Advanced Directives	Enter a description of the directive.
	Advanced Directives	Enter the patient's last name.
	Advanced Directives	Enter the status of the directive.
	Allergy Search	The search criteria revealed no matches.

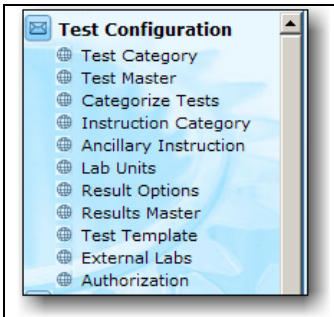
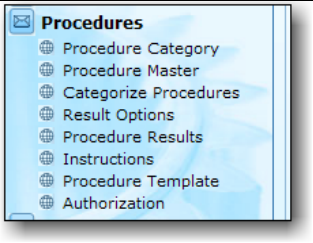
User Errors and Warnings	Location	Resolution
	Allergy Search	Before saving, select an allergy value.
	Add Problem	Before saving select at least one problem.
	Add past surgical history	When using custom procedures, enter the name.

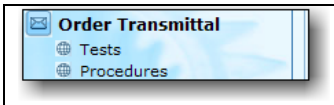
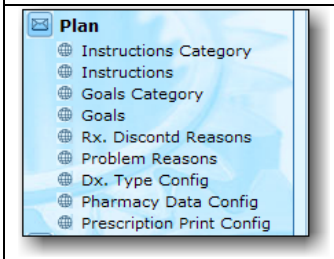
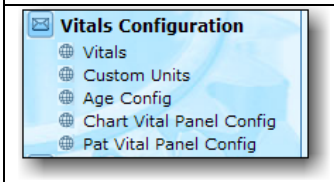
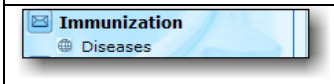
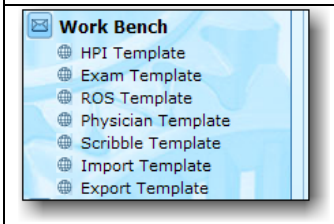
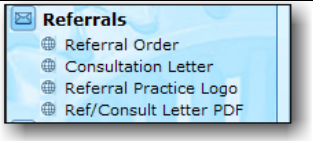
12.0 – EHR User and Practice Setup

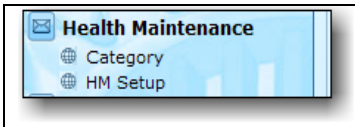
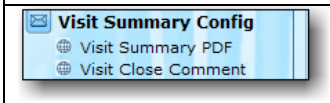
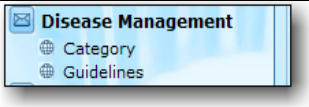
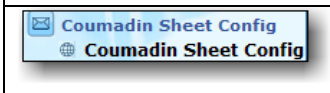
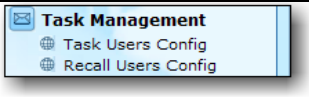
The below list provides users with the location of administrative functions for configuring the EHR.

For help configuring your system, please contact Criterions at 516.466.1942 or at info@criterions.com

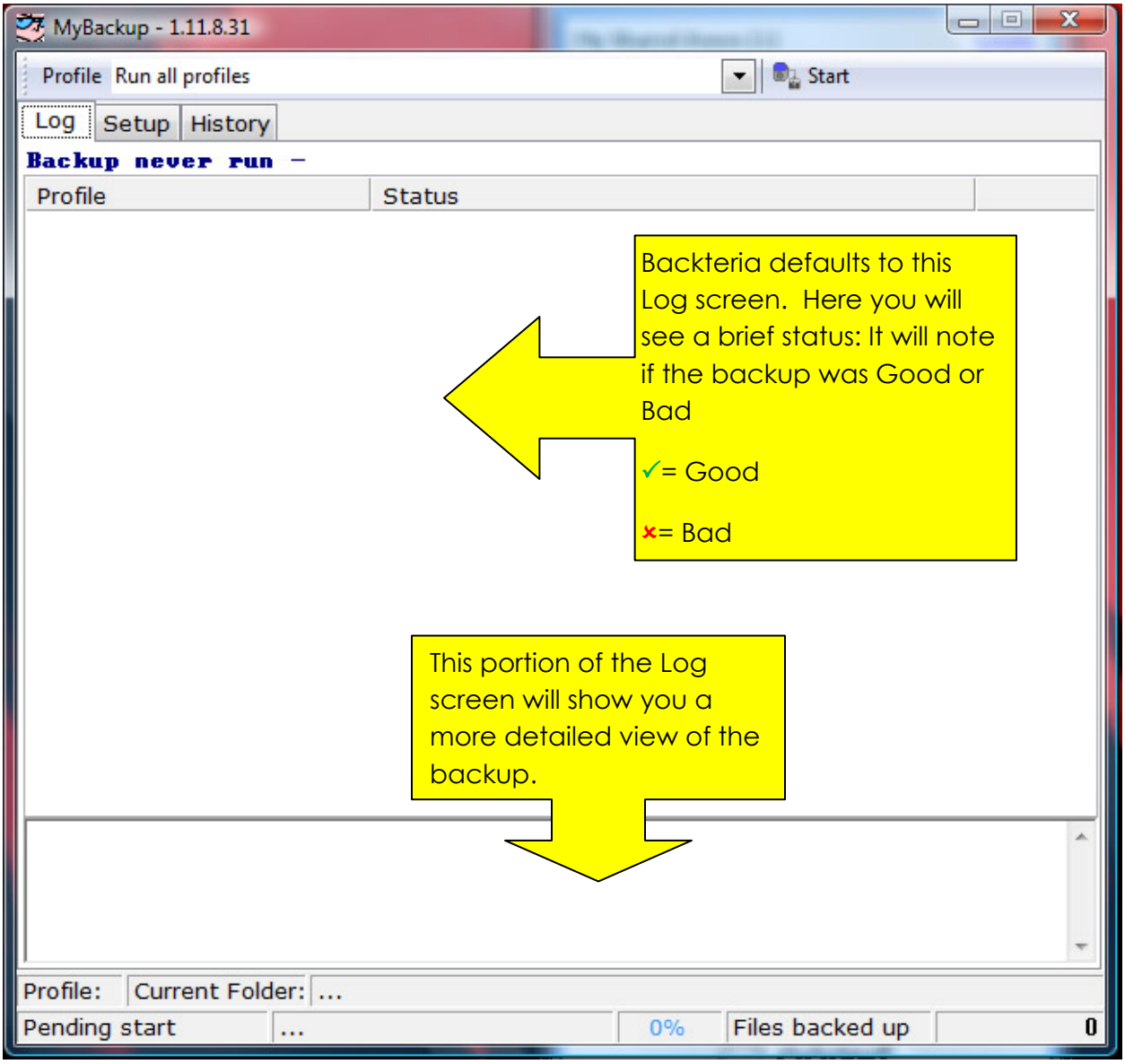


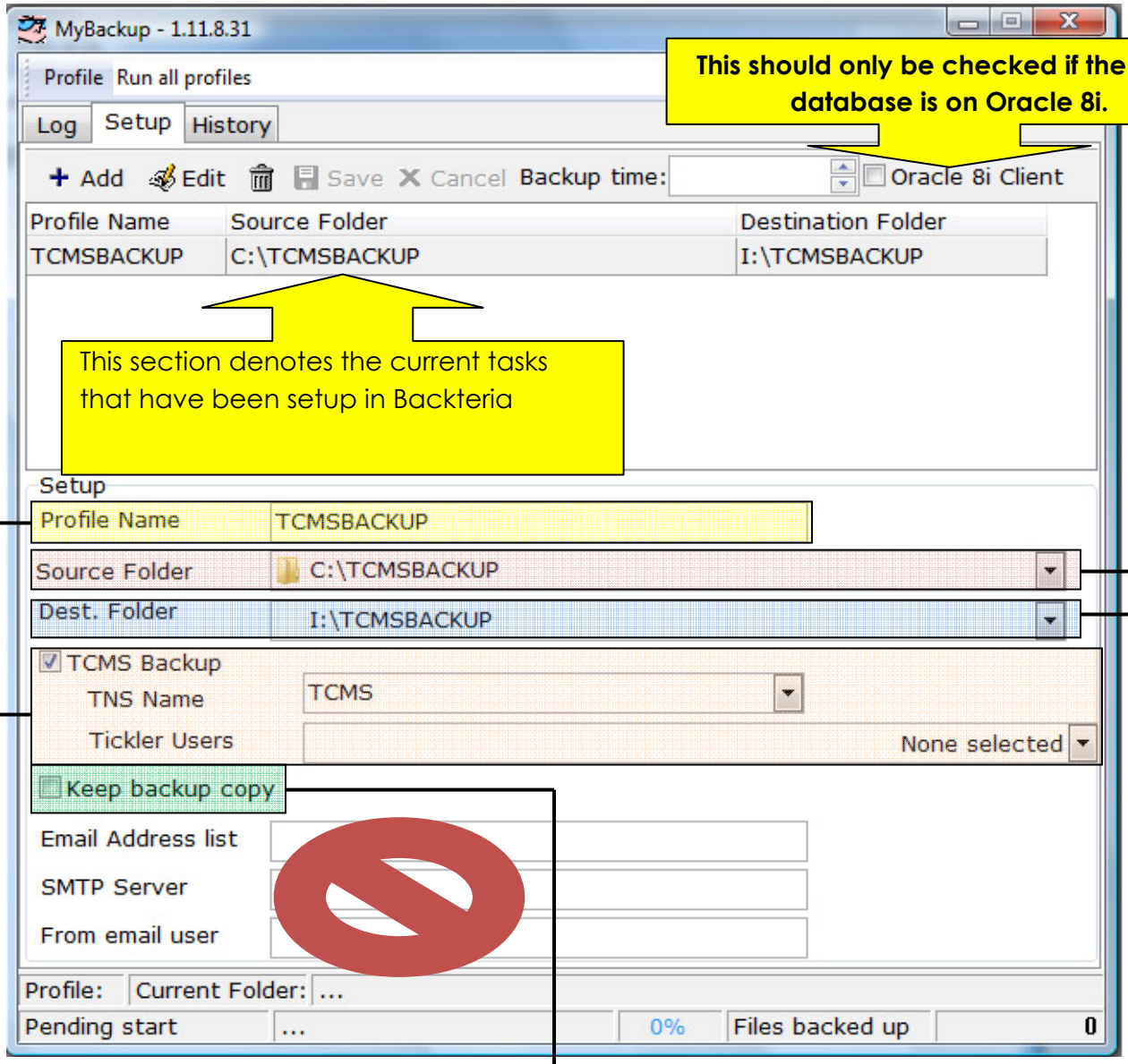
	Test Configuration	Define the values and routing or internal and external labs, including Units, Specimens, and Containers.
	Procedures	Define the results, configuration, instructions and location of procedures.

	Order Transmittal	Create settings for Medication, Test, and Procedure transmittal.
	Plan	Define Instruction, Goals, and Problem and Rx DC reasons.
	History	Create Allergy, Social History, and Family History settings.
	Vitals Configuration	Define the units and ranges for vitals.
	Immunization	Add disease type and doses for immunization.
	Work Bench	Create templates and set defaults for HPI, ROS and Exam.
	Patient Tracker	Setup rooms for placement and tracking of patient visit.
	Print Management	Define printers and routing of print types.
	Referrals	Create/Design referral orders and consultation letters.

	Health Maintenance	Create/Edit Health Maintenance Rules
	System Alerts	Create/Edit System Alerts to be sent to all users.
	User Security	Define EHR users and associations.
	Visit Summary Config	Define File to be created at visit closure and if comments are required.
	Patient Portal Config	Define what aspects should be accessible to patients through secure portal and create Alias text for easier understanding by patient.
	ESB Config	Define if system should automatically create superbill.
	E&M Config	Define override codes and modifiers.
	Disease Management	Create categories and guidelines to display in disease management.
	Intake Sheet Config	Define values to be used with Intake sheet.
	Coumadin Sheet Config	Enable or disable coumadin tracking sheet.
	Task Management	Define users to receive tasks and recalls.

13.0 – System Backup





Name of backup task

This section is only used for TCMS Backups.

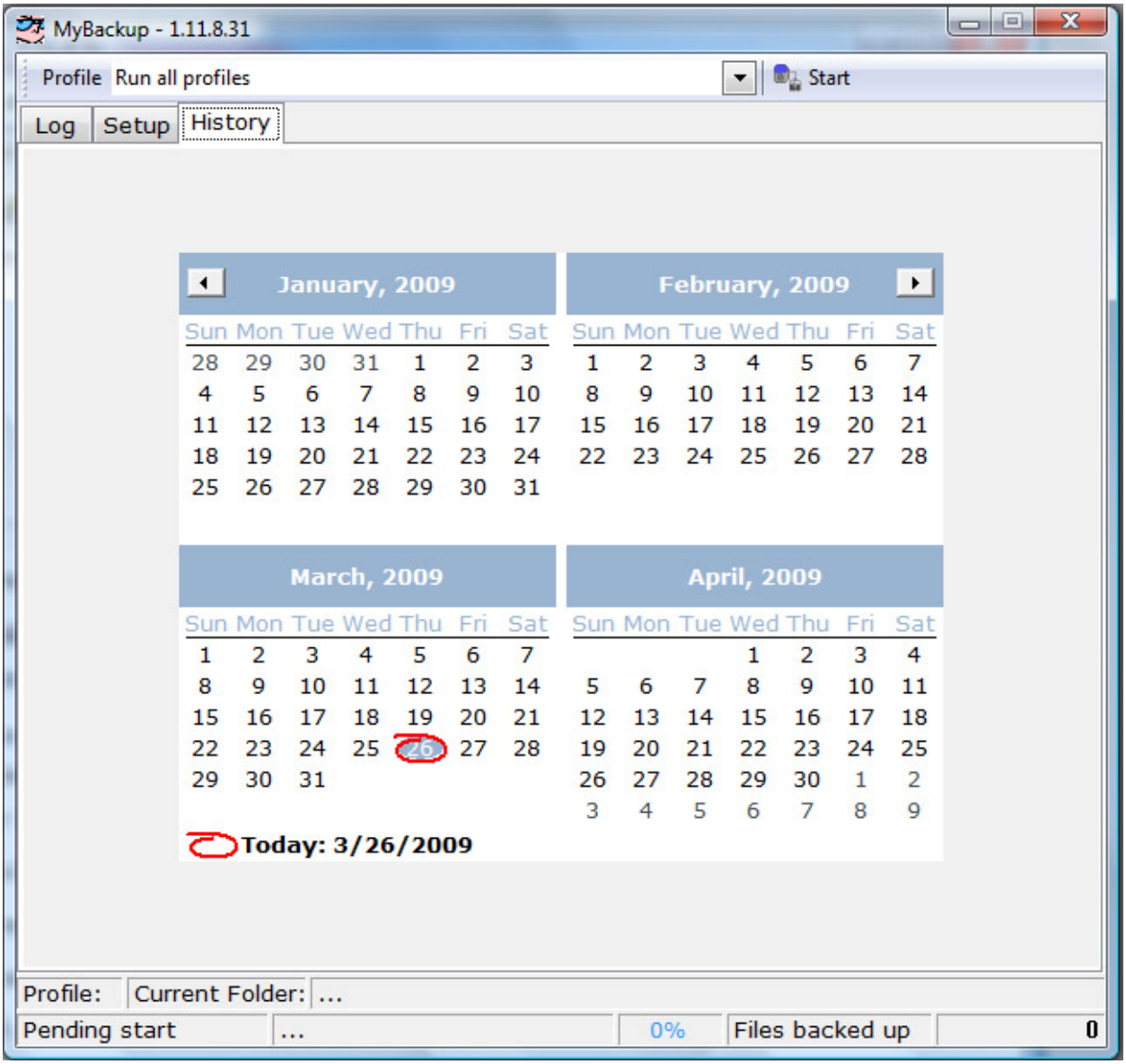
TNS Name: refers to the TNSNAMES.ORA file for Oracle. It ensures that the system connects to the database.

Tickler Users: Utilized to notify any selected user of

Keep backup copy: TCMS exports normally move from the source folder to the destination folder. When this feature is check, the exports are stored locally as well as on the destination

Source Folder: Source Location of desired files for backup.

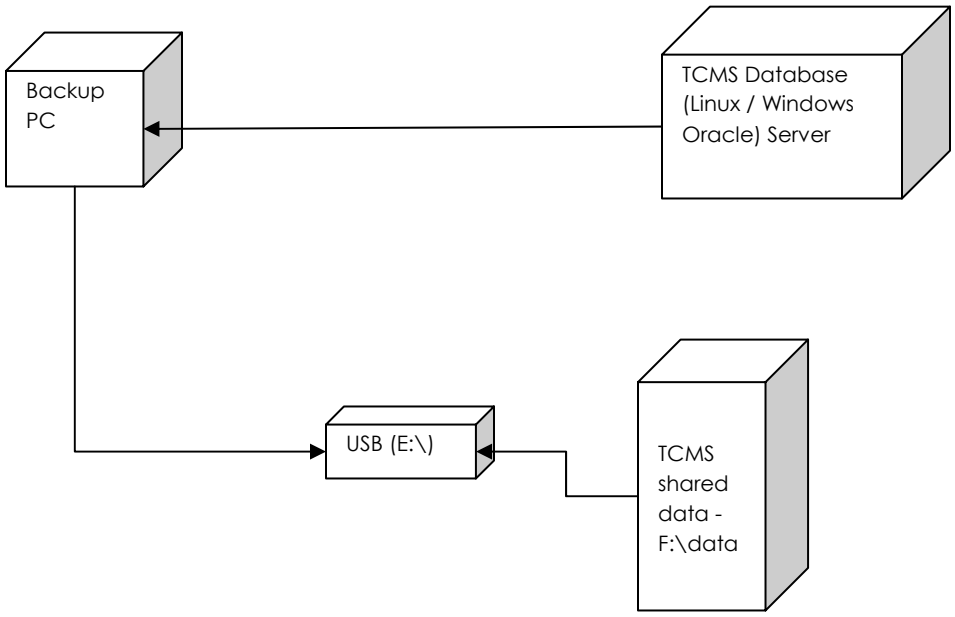
Dest. Folder: Destination location of backup.



The History tab allows users to see a full detailed view of the backup. By double clicking on any day, a log file (txt format) will open. Below is a detailed look at an example log file

File Edit Format View Help

```
3/2/2009 11:05:53 AM: ------------------------------------------------------------------------------
3/2/2009 11:05:53 AM: BACKTERIA version: 1.11.8.31
3/2/2009 11:05:53 AM:
3/2/2009 11:05:53 AM: Starting profile: TCMSBACKUP
3/2/2009 11:05:53 AM: Pruning export file: C:\TCMSBACKUP\\022620091327.TXT
3/2/2009 11:05:53 AM: Pruning export file: C:\TCMSBACKUP\\022620091327_1.EXP
3/2/2009 11:05:53 AM: Backup Disk Free:      445,285.98 MB
3/2/2009 11:05:53 AM: Initiating Oracle Export
3/2/2009 11:05:53 AM: Backup schema: TCMS_DATA Client: [redacted]
3/2/2009 11:05:53 AM: Export Command: EXP system/complex@TCMS
FILE=C:\TCMSBACKUP\030220091105_1.EXP,C:\TCMSBACKUP\030220091105_2.EXP,C:\TCMSBACKUP\030220091105_3.EXP,C:\TCMSBACKUP\030220
091105_4.EXP,C:\TCMSBACKUP\030220091105_5.EXP,C:\TCMSBACKUP\030220091105_6.EXP,C:\TCMSBACKUP\030220091105_7.EXP,C:\TCMSBACKU
P\030220091105_8.EXP,C:\TCMSBACKUP\030220091105_9.EXP,C:\TCMSBACKUP\030220091105_10.EXP,C:\TCMSBACKUP\030220091105_11.EXP,C:
\TCMSBACKUP\030220091105_12.EXP,C:\TCMSBACKUP\030220091105_13.EXP,C:\TCMSBACKUP\030220091105_14.EXP,C:\TCMSBACKUP\0302200911
05_15.EXP,C:\TCMSBACKUP\030220091105_16.EXP,C:\TCMSBACKUP\030220091105_17.EXP,C:\TCMSBACKUP\030220091105_18.EXP,C:\TCMSBACKU
P\030220091105_19.EXP,C:\TCMSBACKUP\030220091105_20.EXP,C:\TCMSBACKUP\030220091105_21.EXP,C:\TCMSBACKUP\030220091105_22.EXP,
C:\TCMSBACKUP\030220091105_23.EXP,C:\TCMSBACKUP\030220091105_24.EXP,C:\TCMSBACKUP\030220091105_25.EXP,C:\TCMSBACKUP\03022009
1105_26.EXP,C:\TCMSBACKUP\030220091105_27.EXP,C:\TCMSBACKUP\030220091105_28.EXP,C:\TCMSBACKUP\030220091105_29.EXP,C:\TCMSBAC
KUP\030220091105_30.EXP,C:\TCMSBACKUP\030220091105_31.EXP,C:\TCMSBACKUP\030220091105_32.EXP,C:\TCMSBACKUP\030220091105_33.EX
P,C:\TCMSBACKUP\030220091105_34.EXP,C:\TCMSBACKUP\030220091105_35.EXP,C:\TCMSBACKUP\030220091105_36.EXP,C:\TCMSBACKUP\030220
091105_37.EXP,C:\TCMSBACKUP\030220091105_38.EXP,C:\TCMSBACKUP\030220091105_39.EXP,C:\TCMSBACKUP\030220091105_40.EXP,C:\TCMSB
ACKUP\030220091105_41.EXP,C:\TCMSBACKUP\030220091105_42.EXP,C:\TCMSBACKUP\030220091105_43.EXP,C:\TCMSBACKUP\030220091105_44.
EXP,C:\TCMSBACKUP\030220091105_45.EXP,C:\TCMSBACKUP\030220091105_46.EXP,C:\TCMSBACKUP\030220091105_47.EXP,C:\TCMSBACKUP\0302
20091105_48.EXP,C:\TCMSBACKUP\030220091105_49.EXP,C:\TCMSBACKUP\030220091105_50.EXP,C:\TCMSBACKUP\030220091105_51.EXP,C:\TCM
SBACKUP\030220091105_52.EXP,C:\TCMSBACKUP\030220091105_53.EXP,C:\TCMSBACKUP\030220091105_54.EXP,C:\TCMSBACKUP\030220091105_5
5.EXP,C:\TCMSBACKUP\030220091105_56.EXP,C:\TCMSBACKUP\030220091105_57.EXP,C:\TCMSBACKUP\030220091105_58.EXP,C:\TCMSBACKUP\03
0220091105_59.EXP,C:\TCMSBACKUP\030220091105_60.EXP,C:\TCMSBACKUP\030220091105_61.EXP,C:\TCMSBACKUP\030220091105_62.EXP,C:\T
CMSBACKUP\030220091105_63.EXP,C:\TCMSBACKUP\030220091105_64.EXP,C:\TCMSBACKUP\030220091105_65.EXP,C:\TCMSBACKUP\030220091105
_66.EXP,C:\TCMSBACKUP\030220091105_67.EXP,C:\TCMSBACKUP\030220091105_68.EXP,C:\TCMSBACKUP\030220091105_69.EXP,C:\TCMSBACKUP\
030220091105_70.EXP,C:\TCMSBACKUP\030220091105_71.EXP,C:\TCMSBACKUP\030220091105_72.EXP,C:\TCMSBACKUP\030220091105_73.EXP,C:
\TCMSBACKUP\030220091105_74.EXP,C:\TCMSBACKUP\030220091105_75.EXP,C:\TCMSBACKUP\030220091105_76.EXP,C:\TCMSBACKUP\0302200911
05_77.EXP,C:\TCMSBACKUP\030220091105_78.EXP,C:\TCMSBACKUP\030220091105_79.EXP,C:\TCMSBACKUP\030220091105_80.EXP,C:\TCMSBACKU
P\030220091105_81.EXP,C:\TCMSBACKUP\030220091105_82.EXP,C:\TCMSBACKUP\030220091105_83.EXP,C:\TCMSBACKUP\030220091105_84.EXP,
C:\TCMSBACKUP\030220091105_85.EXP,C:\TCMSBACKUP\030220091105_86.EXP,C:\TCMSBACKUP\030220091105_87.EXP,C:\TCMSBACKUP\03022009
1105_88.EXP,C:\TCMSBACKUP\030220091105_89.EXP,C:\TCMSBACKUP\030220091105_90.EXP,C:\TCMSBACKUP\030220091105_91.EXP,C:\TCMSBAC
KUP\030220091105_92.EXP,C:\TCMSBACKUP\030220091105_93.EXP,C:\TCMSBACKUP\030220091105_94.EXP,C:\TCMSBACKUP\030220091105_95.EX
P,C:\TCMSBACKUP\030220091105_96.EXP,C:\TCMSBACKUP\030220091105_97.EXP,C:\TCMSBACKUP\030220091105_98.EXP,C:\TCMSBACKUP\030220
091105_99.EXP,C:\TCMSBACKUP\030220091105_100.EXP LOG=C:\TCMSBACKUP\030220091105.TXT FILESIZE=2G DIRECT=Y STATISTICS=NONE
OWNER = (TCMS_DATA,tcms_clientinfo) CONSISTENT=N
3/2/2009 11:12:49 AM: Export Finished
3/2/2009 11:12:49 AM: Log file found
3/2/2009 11:12:49 AM: Oracle Export Successful
3/2/2009 11:12:49 AM: Import Command:
3/2/2009 11:12:49 AM: IMP system/complex@XXX
FILE=C:\TCMSBACKUP\030220091105_1.EXP,C:\TCMSBACKUP\030220091105_2.EXP,C:\TCMSBACKUP\030220091105_3.EXP,C:\TCMSBACKUP\030220
091105_4.EXP,C:\TCMSBACKUP\030220091105_5.EXP,C:\TCMSBACKUP\030220091105_6.EXP,C:\TCMSBACKUP\030220091105_7.EXP,C:\TCMSBACKU
P\030220091105_8.EXP,C:\TCMSBACKUP\030220091105_9.EXP,C:\TCMSBACKUP\030220091105_10.EXP,C:\TCMSBACKUP\030220091105_11.EXP,C:
\TCMSBACKUP\030220091105_12.EXP,C:\TCMSBACKUP\030220091105_13.EXP,C:\TCMSBACKUP\030220091105_14.EXP,C:\TCMSBACKUP\0302200911
05_15.EXP,C:\TCMSBACKUP\030220091105_16.EXP,C:\TCMSBACKUP\030220091105_17.EXP,C:\TCMSBACKUP\030220091105_18.EXP,C:\TCMSBACKU
P\030220091105_19.EXP,C:\TCMSBACKUP\030220091105_20.EXP,C:\TCMSBACKUP\030220091105_21.EXP,C:\TCMSBACKUP\030220091105_22.EXP,
C:\TCMSBACKUP\030220091105_23.EXP,C:\TCMSBACKUP\030220091105_24.EXP,C:\TCMSBACKUP\030220091105_25.EXP,C:\TCMSBACKUP\03022009
1105_26.EXP,C:\TCMSBACKUP\030220091105_27.EXP,C:\TCMSBACKUP\030220091105_28.EXP,C:\TCMSBACKUP\030220091105_29.EXP,C:\TCMSBAC
KUP\030220091105_30.EXP,C:\TCMSBACKUP\030220091105_31.EXP,C:\TCMSBACKUP\030220091105_32.EXP,C:\TCMSBACKUP\030220091105_33.EX
P,C:\TCMSBACKUP\030220091105_34.EXP,C:\TCMSBACKUP\030220091105_35.EXP,C:\TCMSBACKUP\030220091105_36.EXP,C:\TCMSBACKUP\030220
091105_37.EXP,C:\TCMSBACKUP\030220091105_38.EXP,C:\TCMSBACKUP\030220091105_39.EXP,C:\TCMSBACKUP\030220091105_40.EXP,C:\TCMSB
ACKUP\030220091105_41.EXP,C:\TCMSBACKUP\030220091105_42.EXP,C:\TCMSBACKUP\030220091105_43.EXP,C:\TCMSBACKUP\030220091105_44.
EXP,C:\TCMSBACKUP\030220091105_45.EXP,C:\TCMSBACKUP\030220091105_46.EXP,C:\TCMSBACKUP\030220091105_47.EXP,C:\TCMSBACKUP\0302
20091105_48.EXP,C:\TCMSBACKUP\030220091105_49.EXP,C:\TCMSBACKUP\030220091105_50.EXP,C:\TCMSBACKUP\030220091105_51.EXP,C:\TCM
SBACKUP\030220091105_52.EXP,C:\TCMSBACKUP\030220091105_53.EXP,C:\TCMSBACKUP\030220091105_54.EXP,C:\TCMSBACKUP\030220091105_5
5.EXP,C:\TCMSBACKUP\030220091105_56.EXP,C:\TCMSBACKUP\030220091105_57.EXP,C:\TCMSBACKUP\030220091105_58.EXP,C:\TCMSBACKUP\03
0220091105_59.EXP,C:\TCMSBACKUP\030220091105_60.EXP,C:\TCMSBACKUP\030220091105_61.EXP,C:\TCMSBACKUP\030220091105_62.EXP,C:\T
CMSBACKUP\030220091105_63.EXP,C:\TCMSBACKUP\030220091105_64.EXP,C:\TCMSBACKUP\030220091105_65.EXP,C:\TCMSBACKUP\030220091105
_66.EXP,C:\TCMSBACKUP\030220091105_67.EXP,C:\TCMSBACKUP\030220091105_68.EXP,C:\TCMSBACKUP\030220091105_69.EXP,C:\TCMSBACKUP\
030220091105_70.EXP,C:\TCMSBACKUP\030220091105_71.EXP,C:\TCMSBACKUP\030220091105_72.EXP,C:\TCMSBACKUP\030220091105_73.EXP,C:
\TCMSBACKUP\030220091105_74.EXP,C:\TCMSBACKUP\030220091105_75.EXP,C:\TCMSBACKUP\030220091105_76.EXP,C:\TCMSBACKUP\0302200911
05_77.EXP,C:\TCMSBACKUP\030220091105_78.EXP,C:\TCMSBACKUP\030220091105_79.EXP,C:\TCMSBACKUP\030220091105_80.EXP,C:\TCMSBACKU
P\030220091105_81.EXP,C:\TCMSBACKUP\030220091105_82.EXP,C:\TCMSBACKUP\030220091105_83.EXP,C:\TCMSBACKUP\030220091105_84.EXP,
C:\TCMSBACKUP\030220091105_85.EXP,C:\TCMSBACKUP\030220091105_86.EXP,C:\TCMSBACKUP\030220091105_87.EXP,C:\TCMSBACKUP\03022009
1105_88.EXP,C:\TCMSBACKUP\030220091105_89.EXP,C:\TCMSBACKUP\030220091105_90.EXP,C:\TCMSBACKUP\030220091105_91.EXP,C:\TCMSBAC
KUP\030220091105_92.EXP,C:\TCMSBACKUP\030220091105_93.EXP,C:\TCMSBACKUP\030220091105_94.EXP,C:\TCMSBACKUP\030220091105_95.EX
P,C:\TCMSBACKUP\030220091105_96.EXP,C:\TCMSBACKUP\030220091105_97.EXP,C:\TCMSBACKUP\030220091105_98.EXP,C:\TCMSBACKUP\030220
091105_99.EXP,C:\TCMSBACKUP\030220091105_100.EXP LOG=C:\TCMSBACKUP\IMP_030220091105.TXT FILESIZE=2G FULL= Y
3/2/2009 11:12:49 AM: Note: Change the "XXX" to the new TNS name
3/2/2009 11:12:49 AM: Copying Exports to USB drive
3/2/2009 11:12:49 AM: All exports copid to USB device
3/2/2009 11:12:49 AM: Backup profile completed.
```



Process of backup:

1. TCMS data from TCMS Database Server (Either Linux or Windows Server) is exported to the local drive (C:\) of the Backup PC – stored in C:\TCMSBACKUP.
2. Backup software (Backteria) then begins process of backing up data to the USB Hard Drive (E:\).
3. Shared Appliance (F:\Data) then begins backup to USB Device (Data backups are not recommended with Backteria. The software was designed initially for TCMS).

14.0 – Remote Support

Should you require assistance from Criterions where it is necessary for Criterions staff to connect to a computer remotely, the connection is based on rights determined as secure by your system administrator. If your application is setup to be accessed over the internet using aforementioned protocols, the Criterions Staff may provide support by using an administrative level account present in all instances of the application. The client is encouraged to allow SSH access to their database for update purposes, we may also choose to host the application locally and pull the data from their site to assist in troubleshooting. Other support options include 3rd party utilities such as Symantec PcAnywhere or web based services such as GoToMeeting.

	Remote Support protocols are left to the discretion of the client system administrators.

15.0 – User Setup, Rights, Passwords and Audits

15.1 – Accessing Setup

1. Open the **Criterions TCMS Practice Management System**
2. Click **File -> Setup** (Figure 1).

Note: A user must have administrative rights to access the Practice Management Setup.

The Practice Setup Options List will appear (Figure 2).

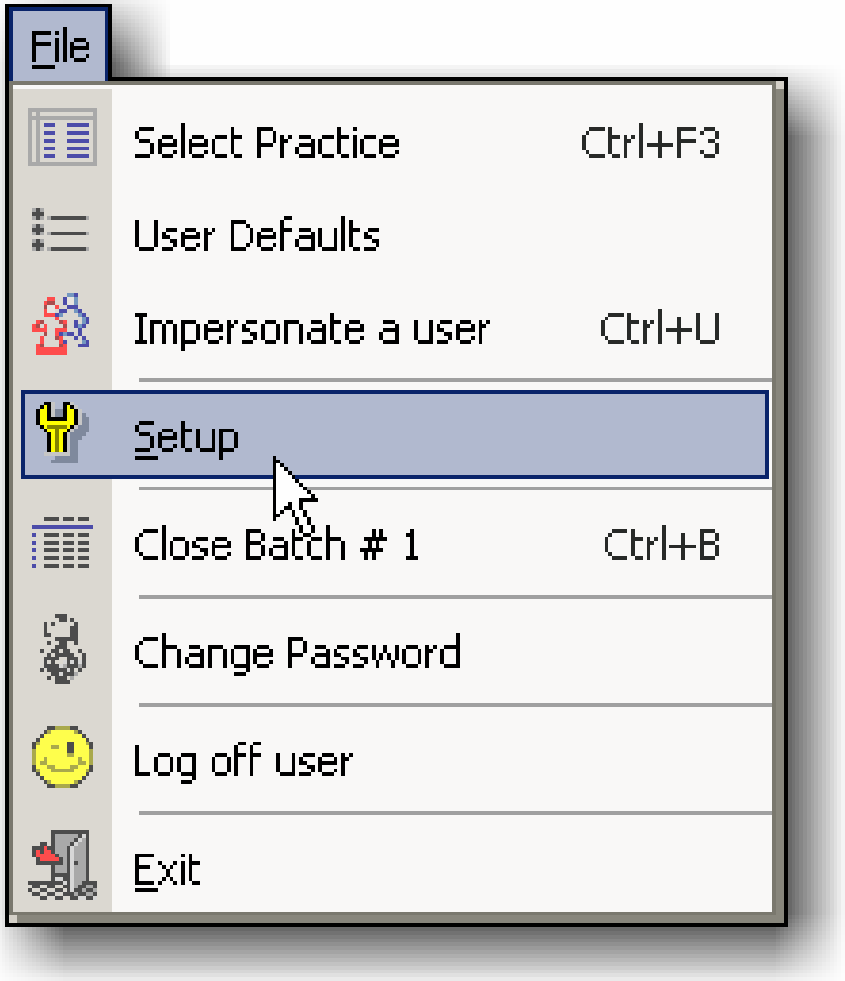


Figure 1

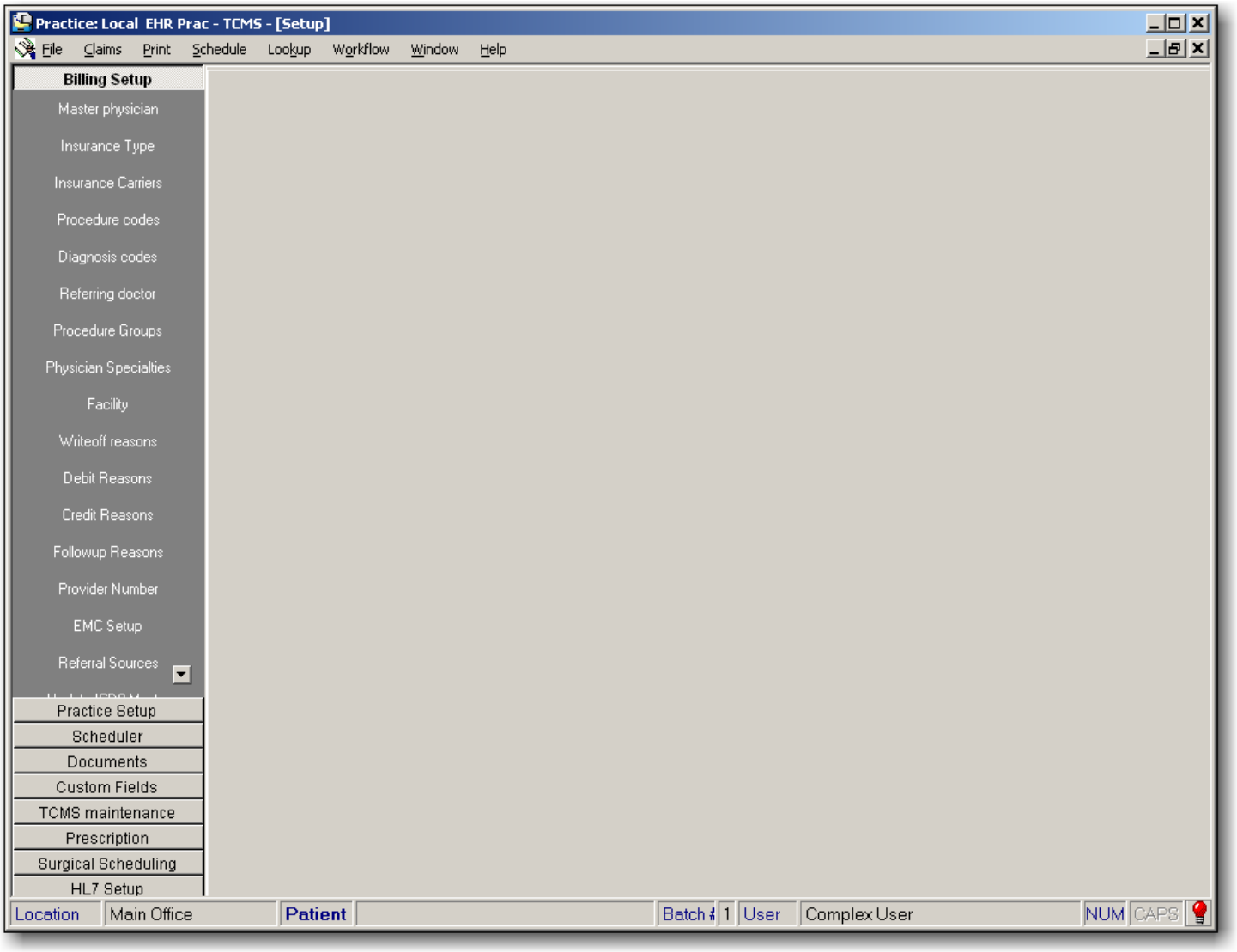


Figure 2

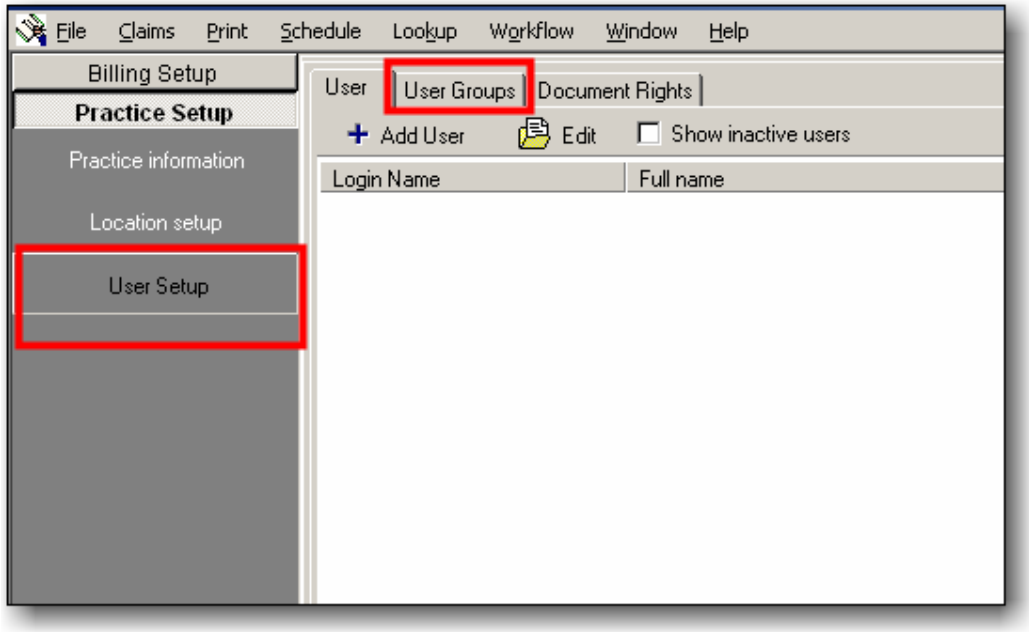
Create a User Group

Before creating a user in the Criterions TCMS Practice Management System a Group should be created. Groups allow administrators to manage the rights of all users in the group without changing individual user profiles. A group can have any number of users as designated by the practice.

Figure 3

1. From the Setup menu, click **Practice Setup** (Figure 3).
2. Click **User Setup.**

A list of active users will appear.



3. Click the **User Groups** tab.

Note: Adding a user without groups will allow for a user to be given two options for system rights: Administrator or No Rights.

Figure 4

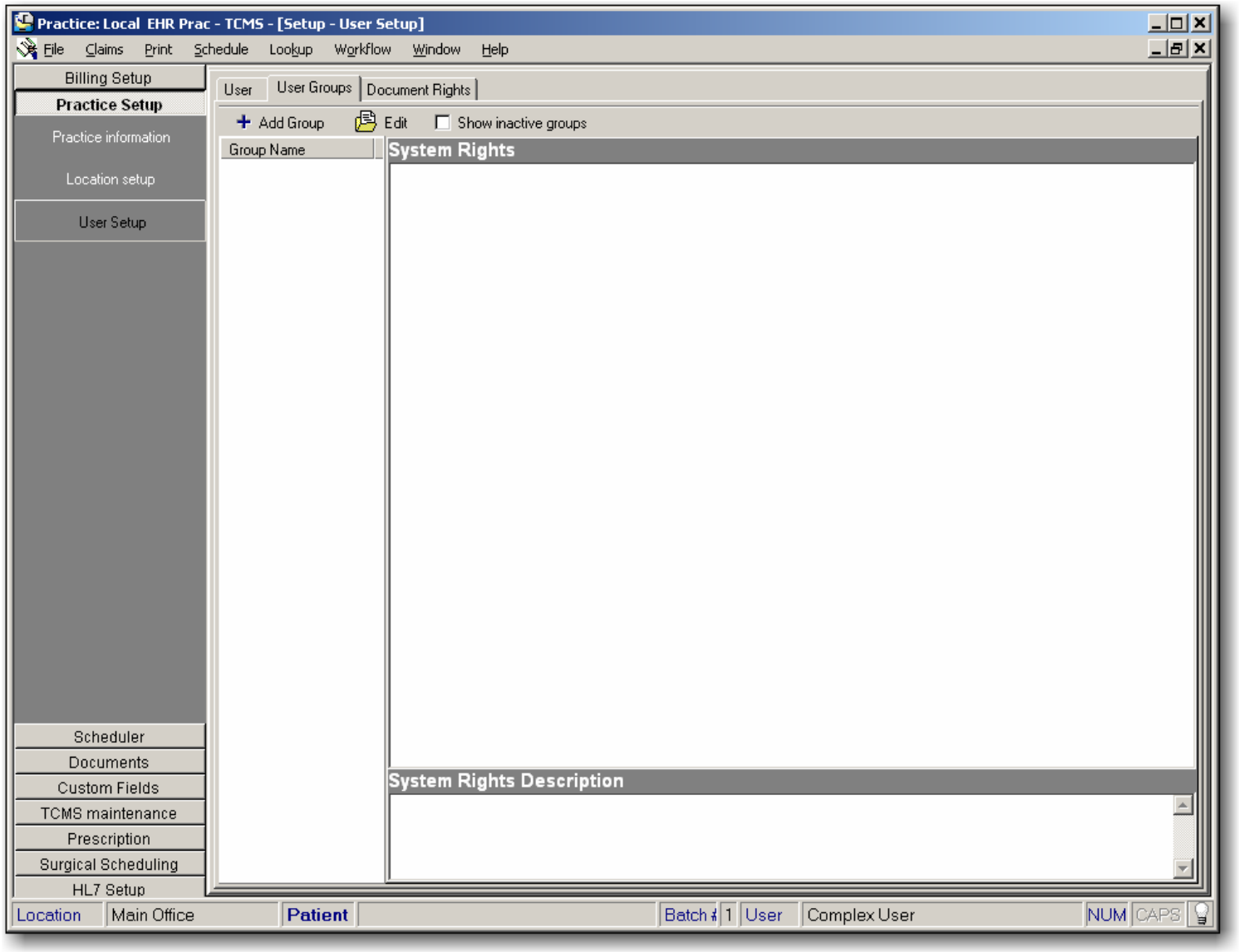

Practice: Local EHR Prac - TCMS - [Setup - User Setup]
File
Claims
Print
Schedule
Lookup
Workflow
Window
Help
Billing Setup
Practice Setup
Practice information
Location setup
User Setup
Scheduler
Documents
Custom Fields
TCMS maintenance
Prescription
Surgical Scheduling
HL7 Setup
User
User Groups
Document Rights
Add Group
Edit
Show inactive groups
Group Name
System Rights
System Rights Description
Location
Main Office
Patient
Batch #
1
User
Complex User
NUM
CAPS

Figure 5

A list of any active groups will appear.

4. Click [+ Add Group].

5. Enter a **GROUP NAME** in the displayed Pop-Up.
6. Click [OK]

Note: Group names should be easily identifiable and created with the understanding that all group members will have equivalent system rights.

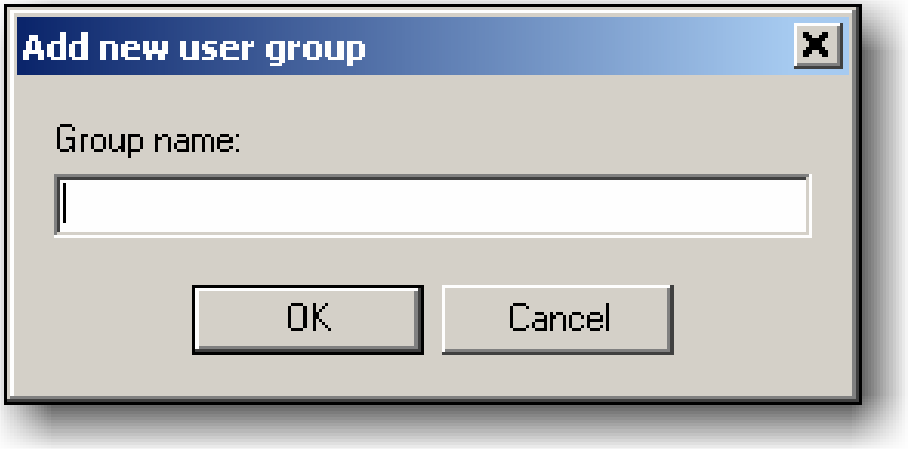


Figure 6

The added group names display in the left hand column.

7. Click on the **GROUP NAME** you would like to edit.

In this example, a user has created groups labeled as *Frontdesk*, *Nurse*, and *Physician*.

Next, the user will give each group distinct rights and then place users into the groups.

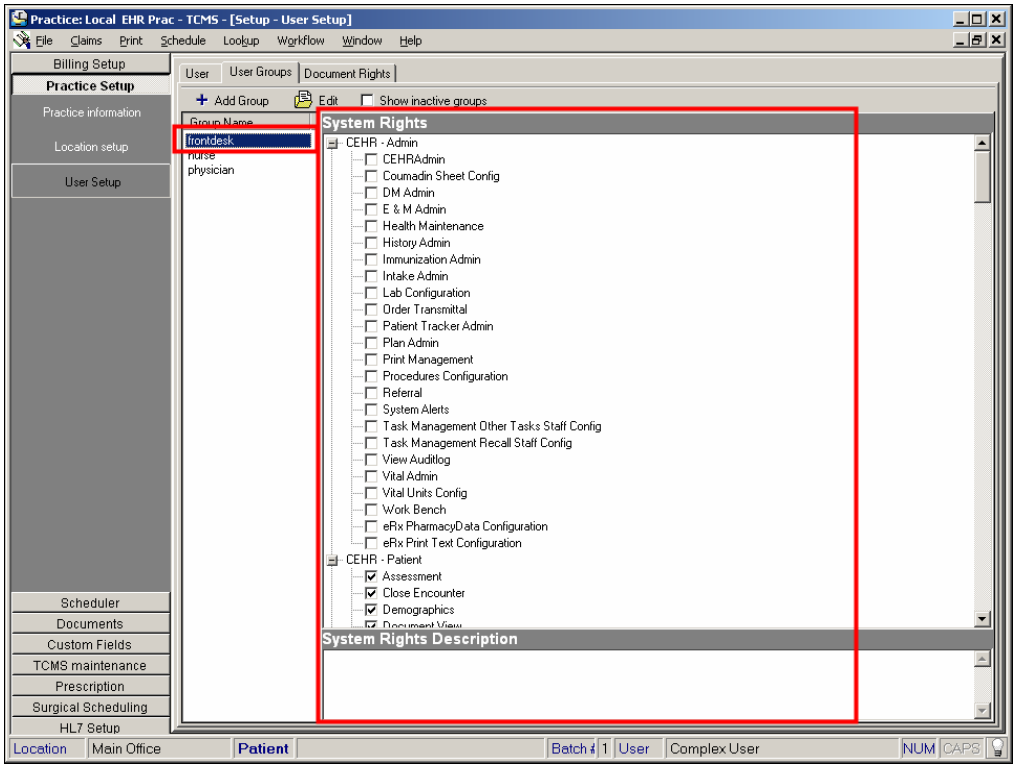


Figure 7

The system admin can choose what operations and access should be given to users of a particular group. If a group does not have an item selected they will not be able to perform the associated function.

8. Select the **GROUP NAME** and modify appropriate functions.
9. Click the **USER** tab.

Note: There is no save button on these screens. Once you click an option it is automatically added to that group profile.

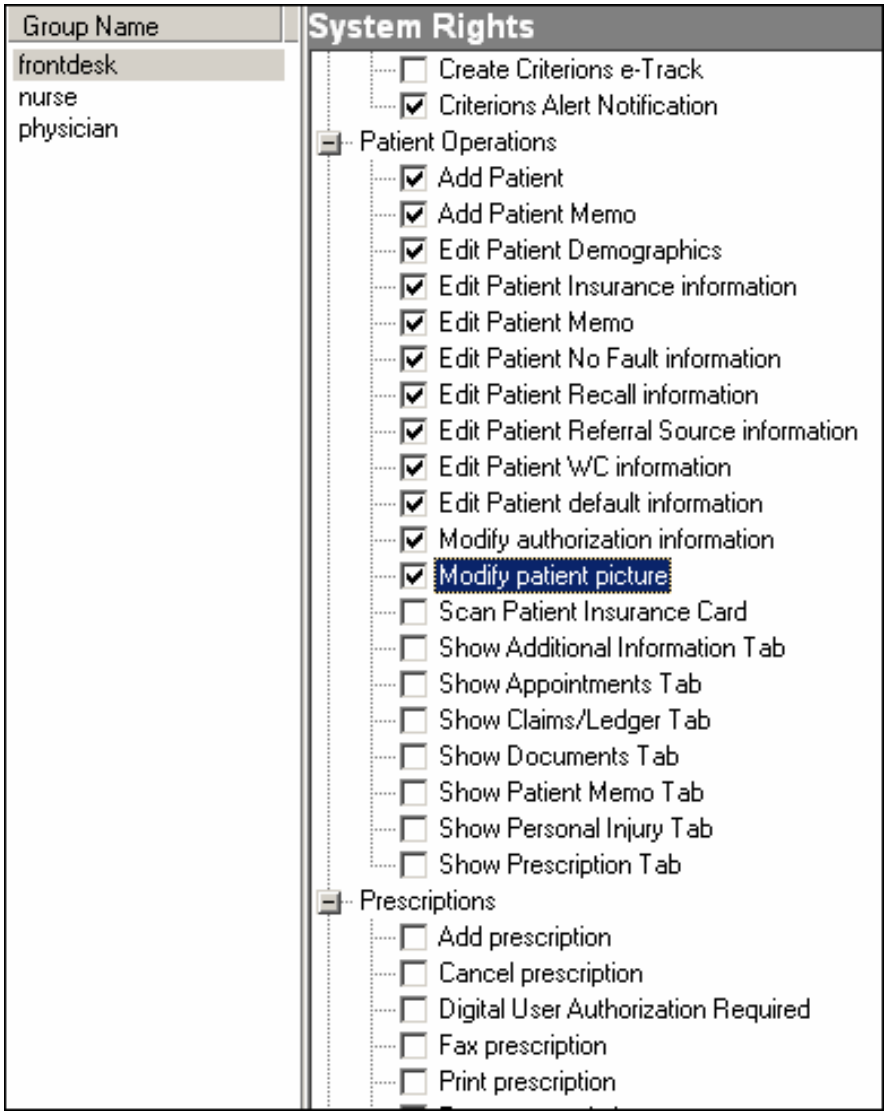


Figure 8

10. Click

.

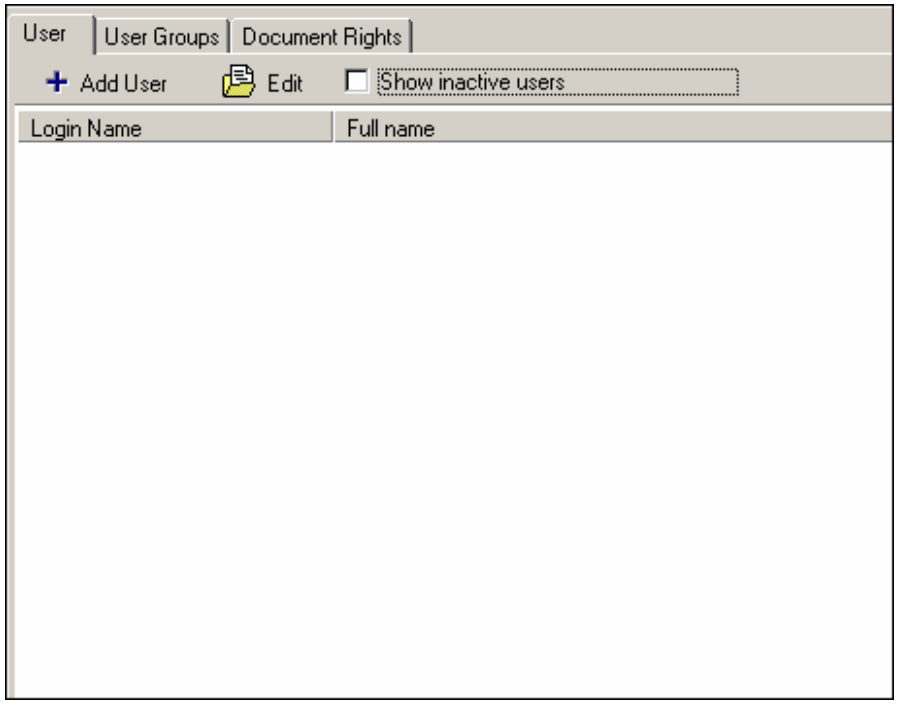
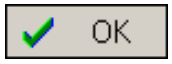


Figure 9

The User Setup screen will appear.

11. Enter a **LOGIN NAME** for the user.
12. Enter the users **FULL NAME**.

In the Group Rights list will show the two default settings, No Rights and Administrator, as well as the custom groups you have created. These Group Rights will be displayed for every location that the practice has setup. This allows users to have one set of rights at one location and another set of rights at another.

13. Select the **GROUP RIGHTS** for this user at each location.
14. Click 

The user has been created and given rights.

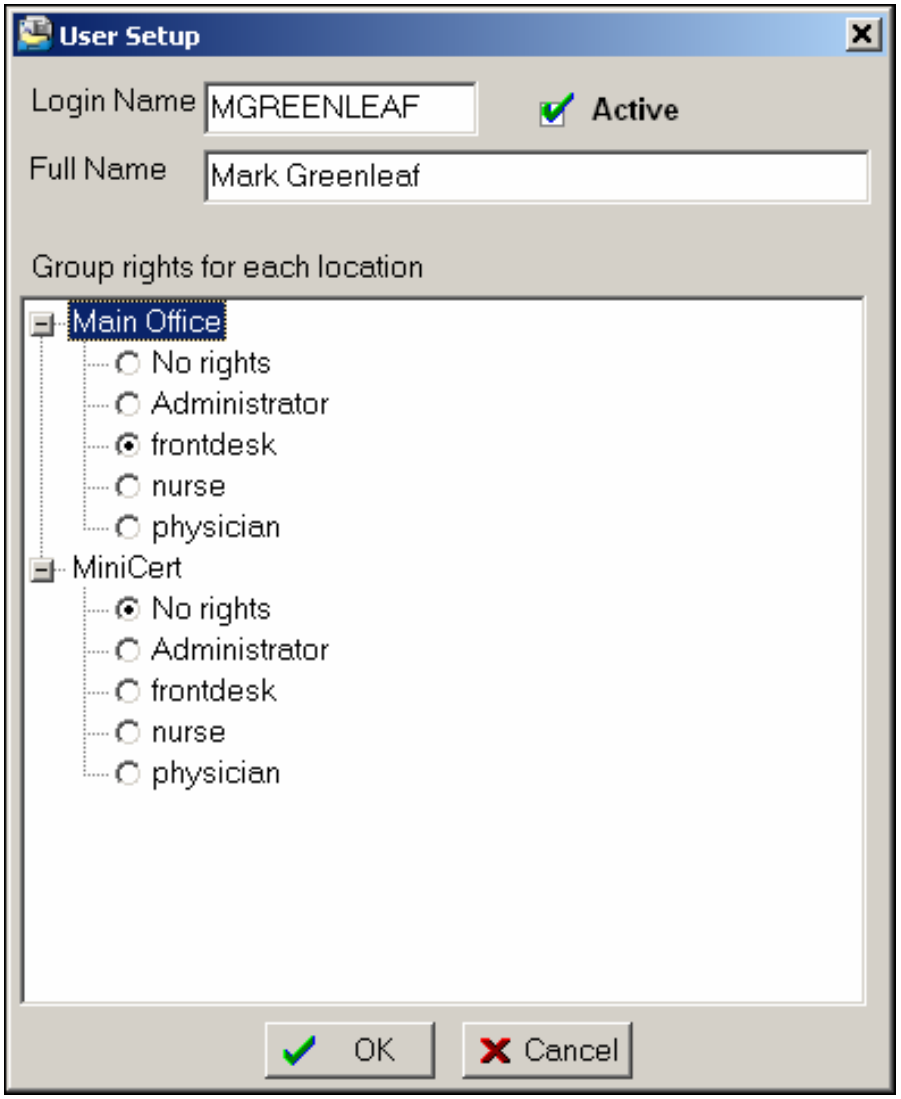


Figure 10

Modify Existing User Accounts

Once a user account has been added it will display in the User list.

Editing users consist of two parts.

1. Editing the User Groups they belong to
2. Editing the rights the Group has.

In the first scenario we will edit the Groups to which a user belongs.

1. Double-Click on the name of the user you would like to edit.

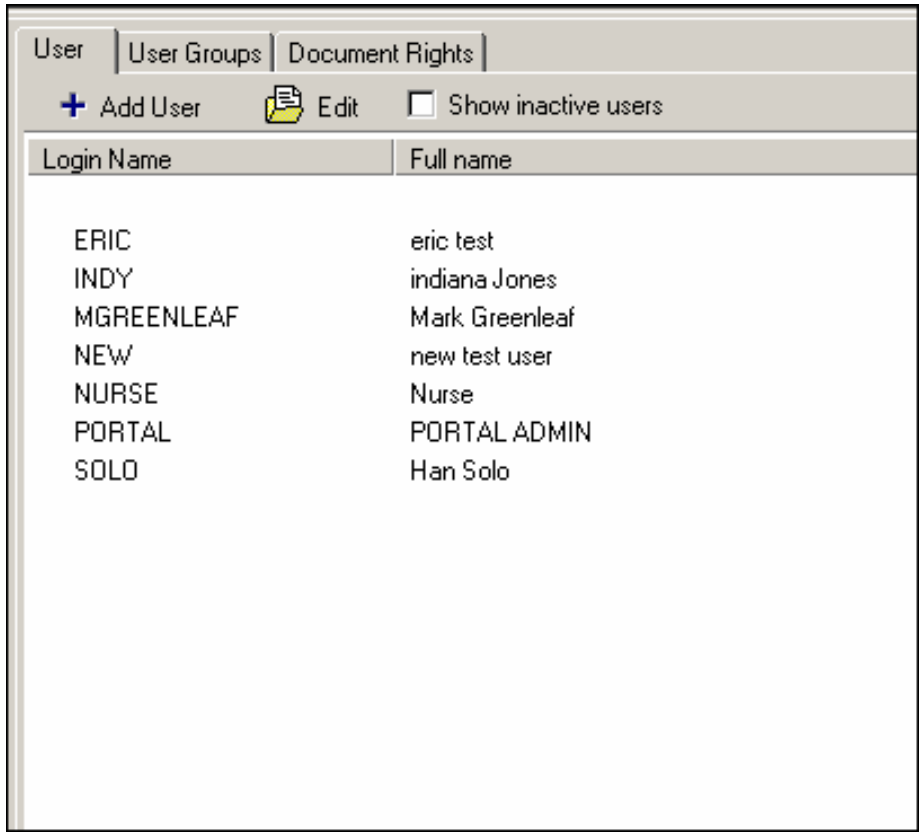


Figure 11

The user's current user rights are displayed.

User Mark Greenleaf has become an administrator for the Main Office.

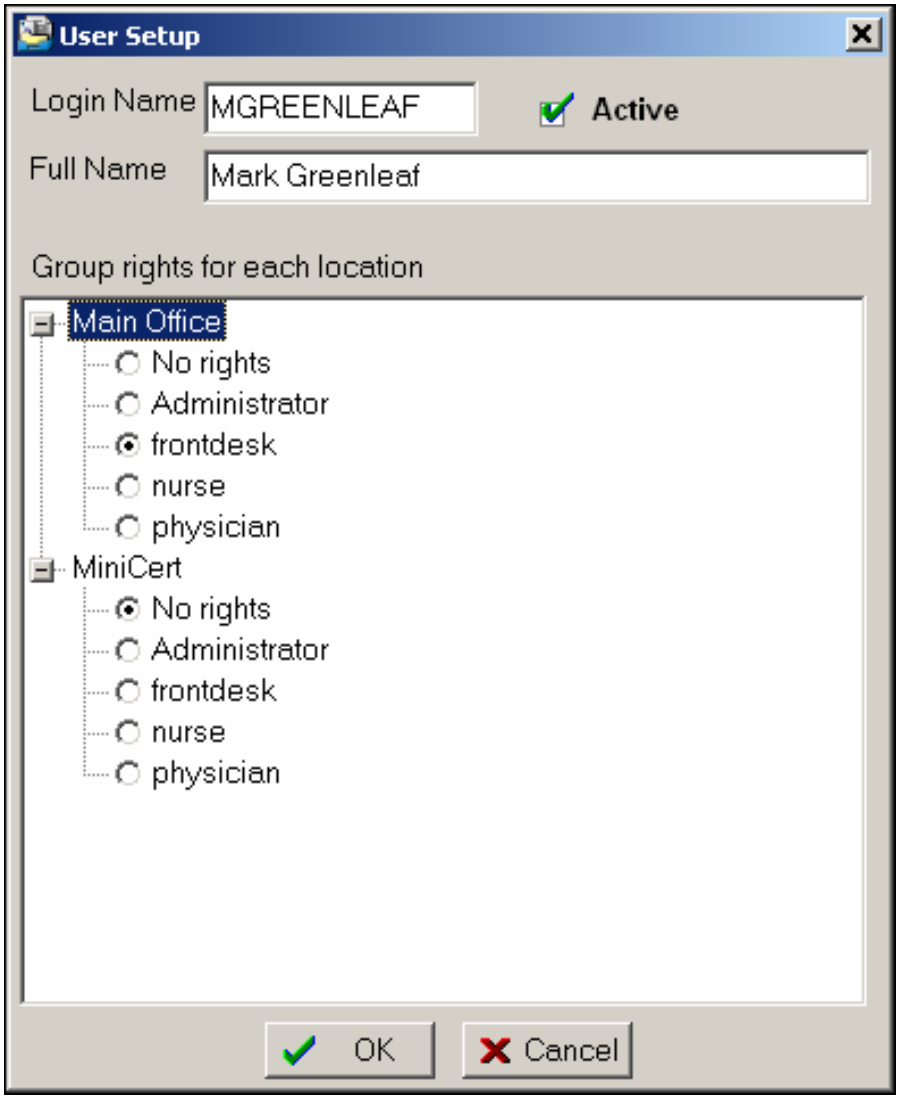


Figure 12

2. Select the **ADMINISTRATOR** for the Main Office Location.
3. Click ✔ OK

The user's system rights will now reflect the settings for an administrator in the Main Office Location.

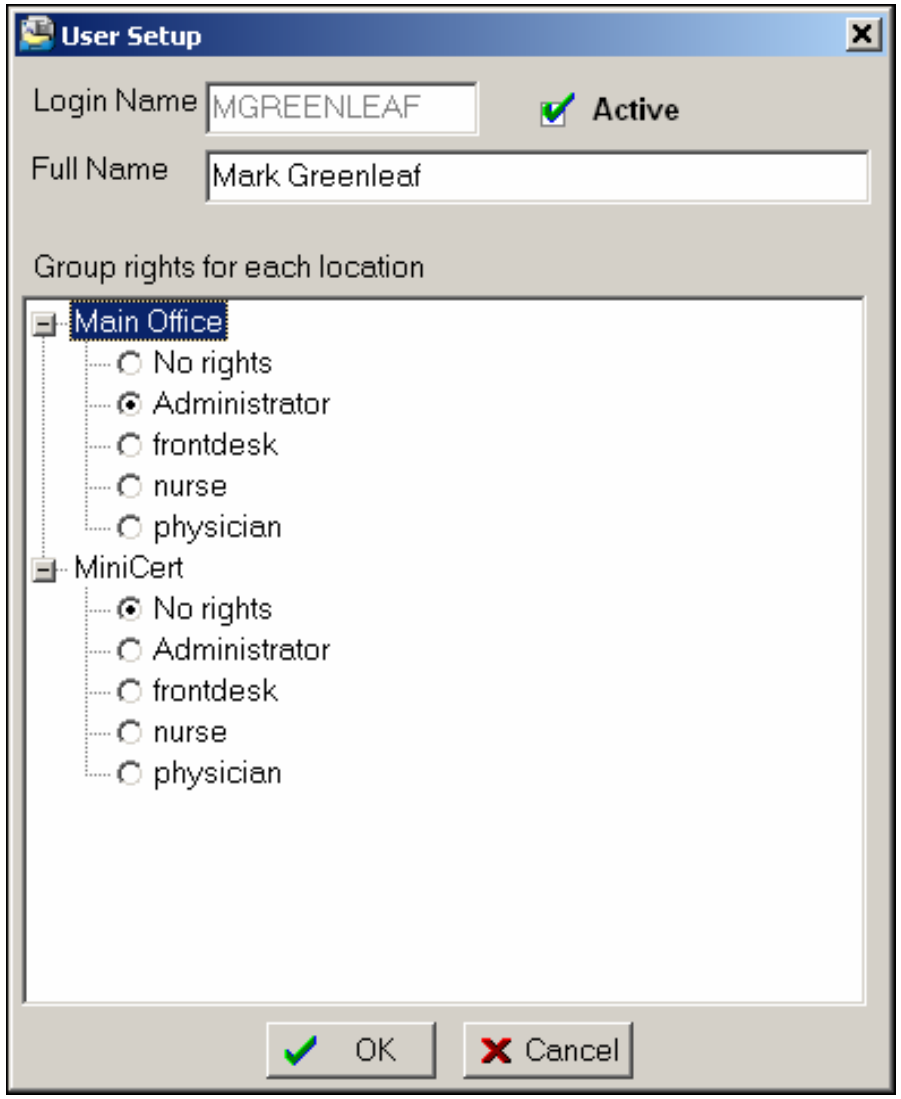


Figure 13

If a user needs a change in system rights there is an important distinction that must be made. Do the changes required for

the user apply to ALL members of the group they belong to.

In this scenario, we will edit the rights of the frontdesk group to allow all front desk members to scan insurance cards.

4. Click on the **USER GROUPS** tab.

The added group names display in the left hand column.

5. Click on the **GROUP NAME** you would like to edit.

In this example, we are editing the rights for the Frontdesk group.

A list of group rights displays.

Figure 14

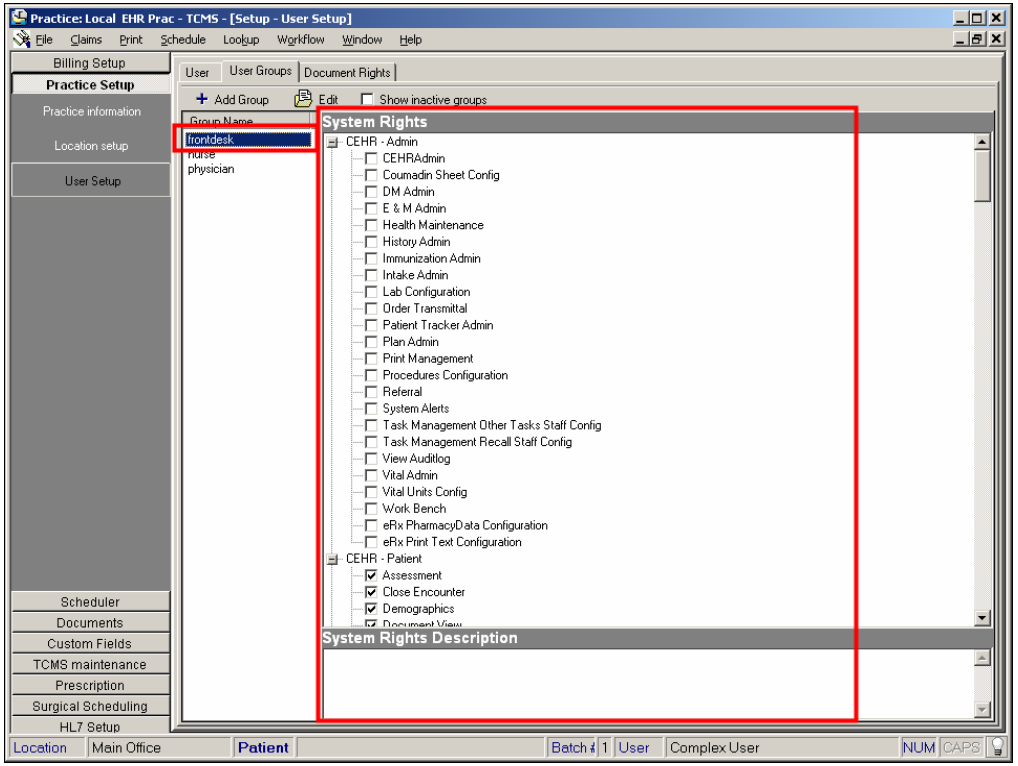


Figure 15

6. Scroll down to find the right you want to edit.

In this scenario insurance card scanning rights are to be given to all members of the front desk group.

7. Check the box before "Scan Patient Insurance Card."

All users across all locations who are given *Frontdesk* group rights will now have the ability to scan Patient Insurance Cards.

If a user is a member of a group and needs rights that should not be given to the additional group members, a new group should be added and the user moved to that group.

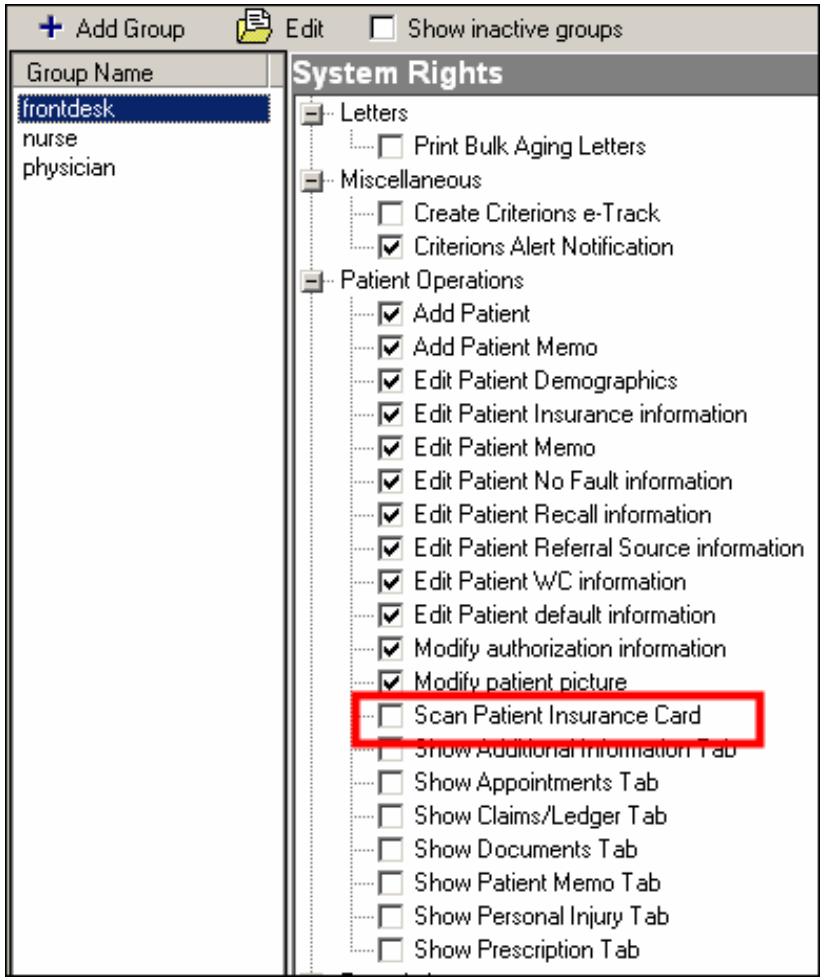


Figure 16

Deactivate a User Account

Should a user be removed from the system completely, the system administrator can Inactivate the user account.

1. Open the **Criterions TCMS Practice Management System**

2. Click **File -> Setup** (Figure 17).

Note: A user must have administrative rights to access the Practice Management Setup.

The Practice Setup Options List will appear (Figure 2).

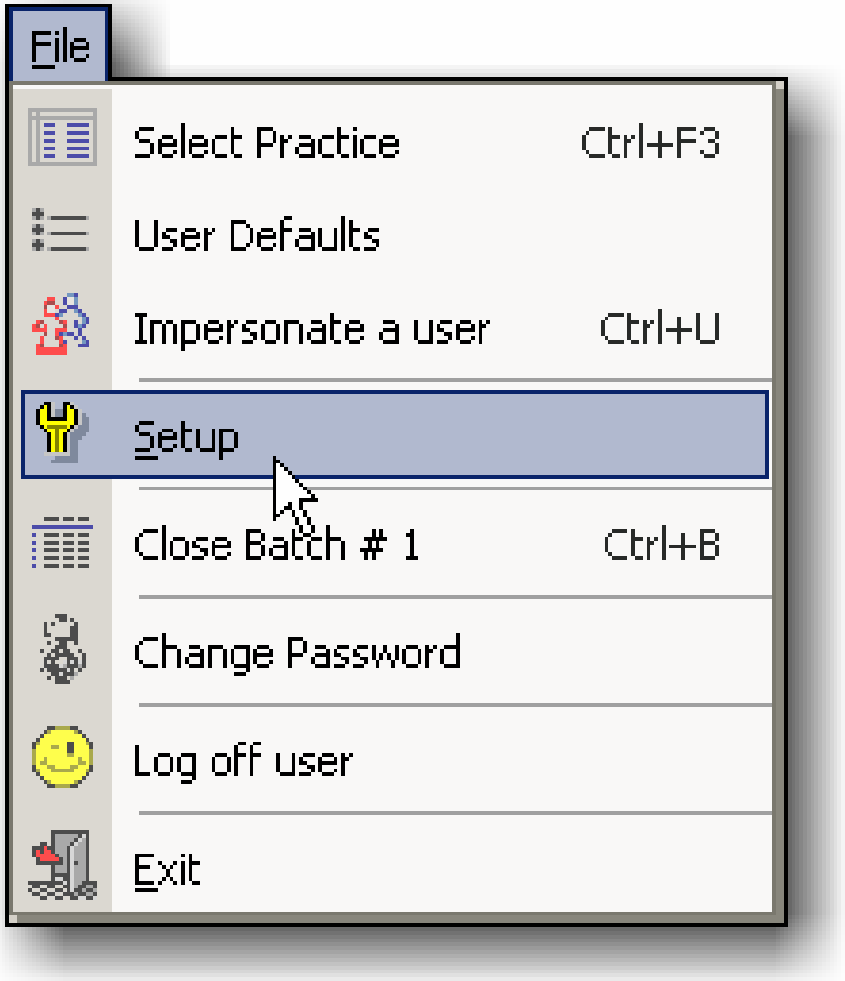


Figure 17

3. From the Setup menu, click **Practice Setup** (Figure 3).
4. Click **User Setup.**

Figure 18

Once a user account has been added it will display in the User list.

5. Double-Click on the name of the user you would like to edit.

In this scenario we are going to inactivate the account for MGREENLEAF.

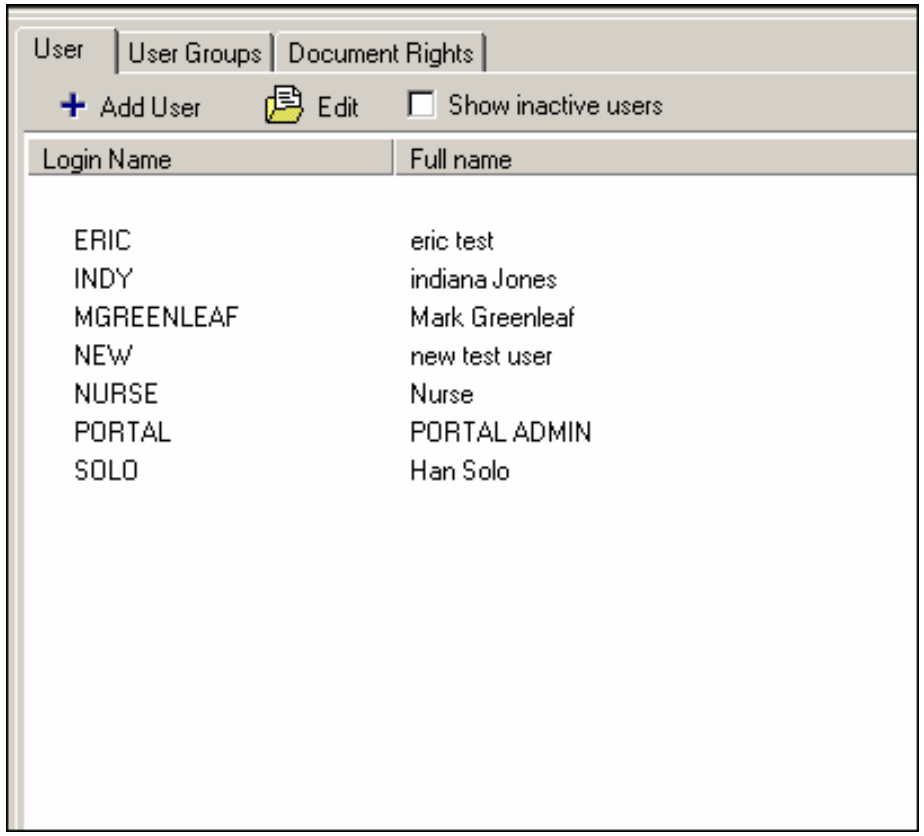


Figure 19

Currently the User Setup shows a green check mark in the Active box.

6. Uncheck the **Active** box.

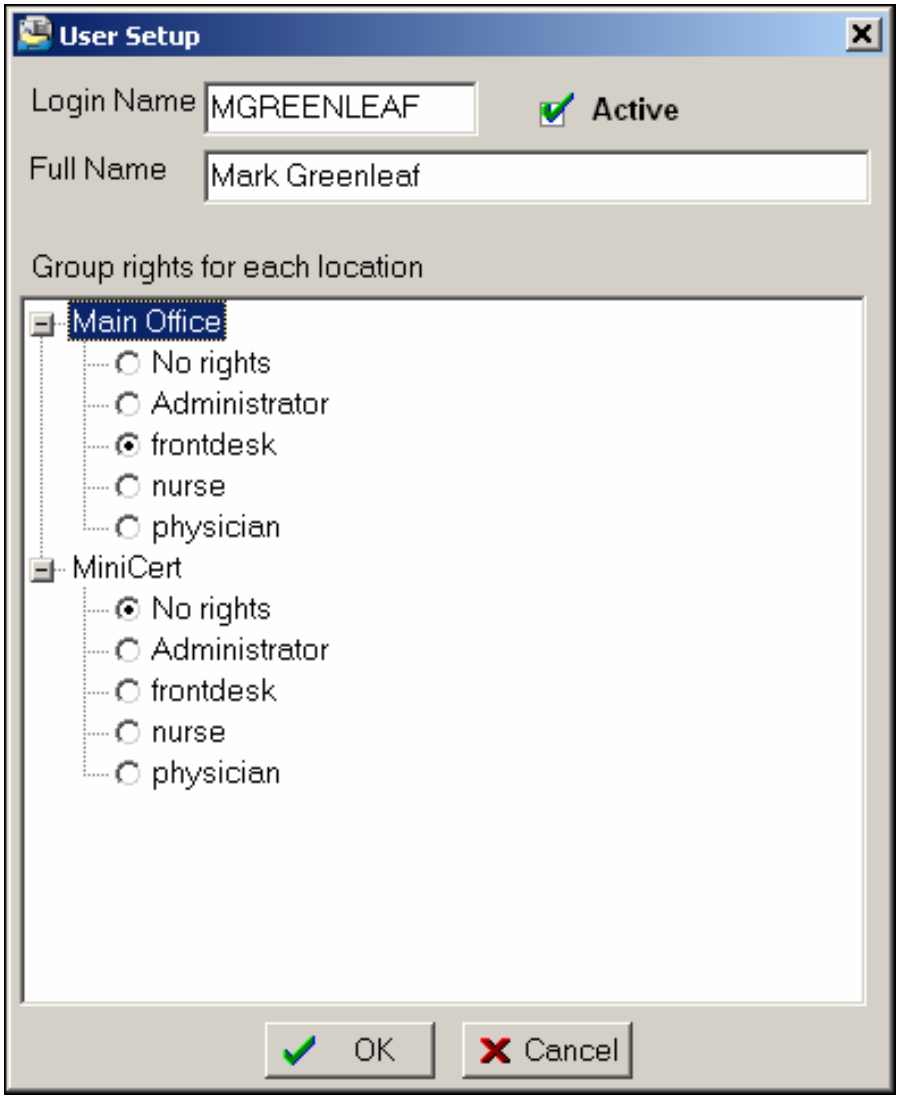


Figure 20

7. Click OK

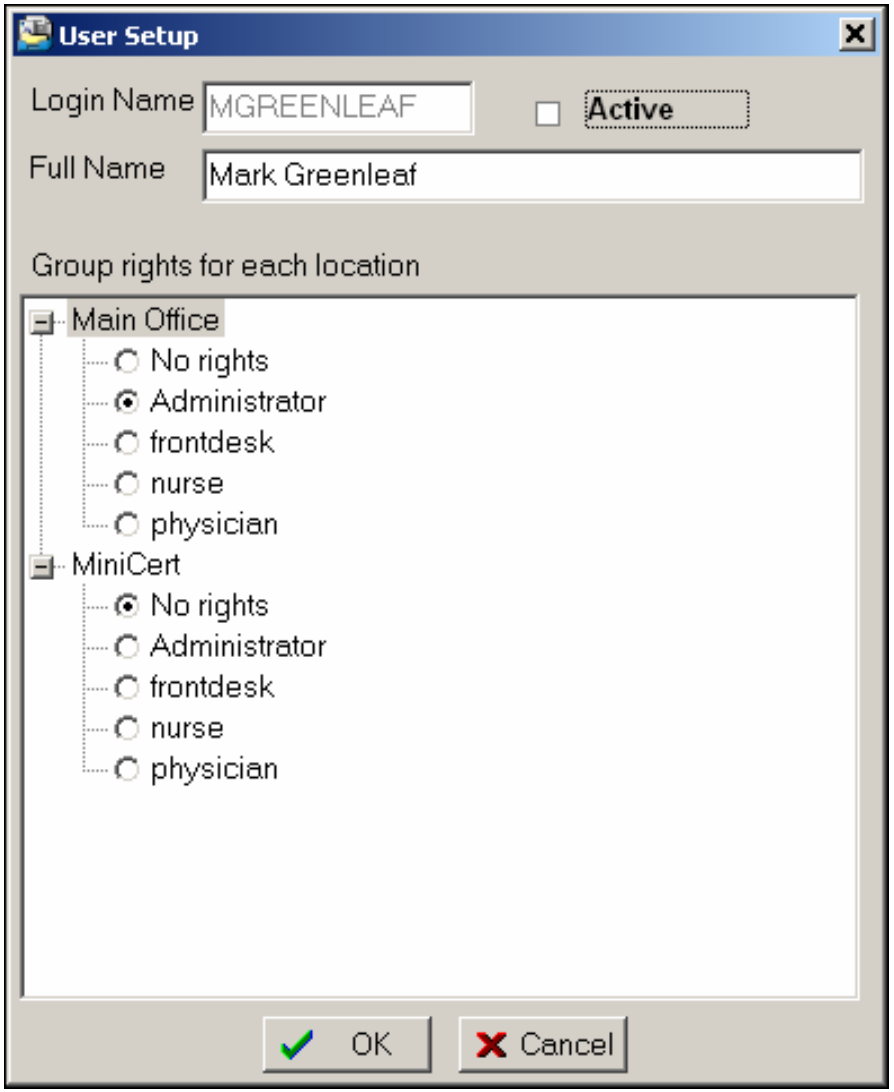


Figure 21

The user is now removed from the User list.

Note: No record is permanently deleted. The user account has been inactivated.

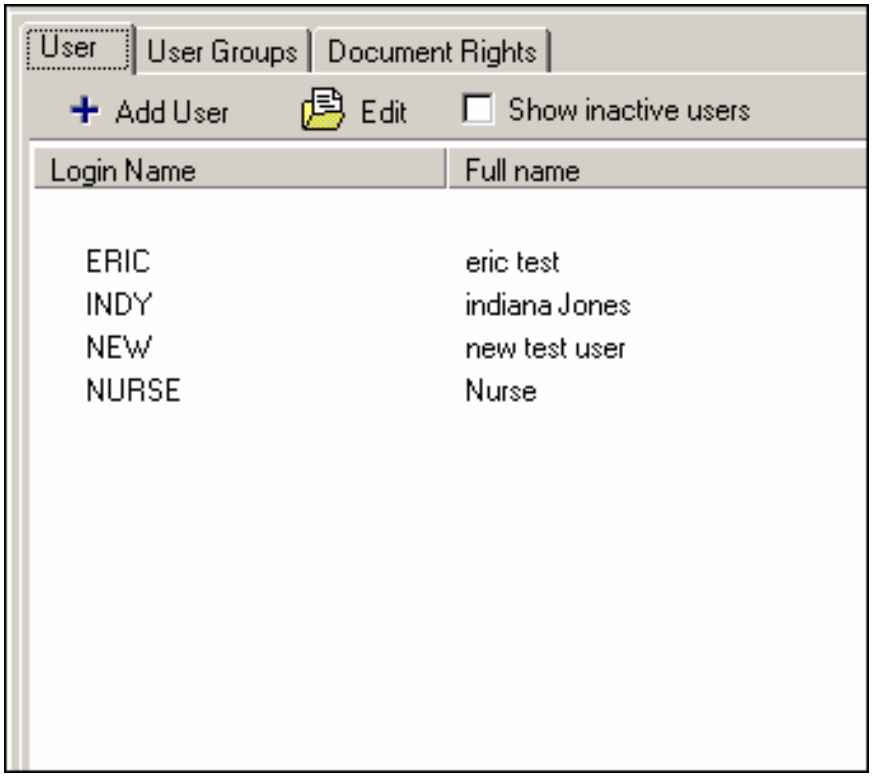


Figure 22

8. Click the check box to "Show inactive users".

Figure 23

The complete list of users, active and inactive are displayed.

The inactive users are designated by a flag symbol beside the name.

To re-activate an inactive account access the user setup screen,

9. Double-Click on the user name to reactivate.

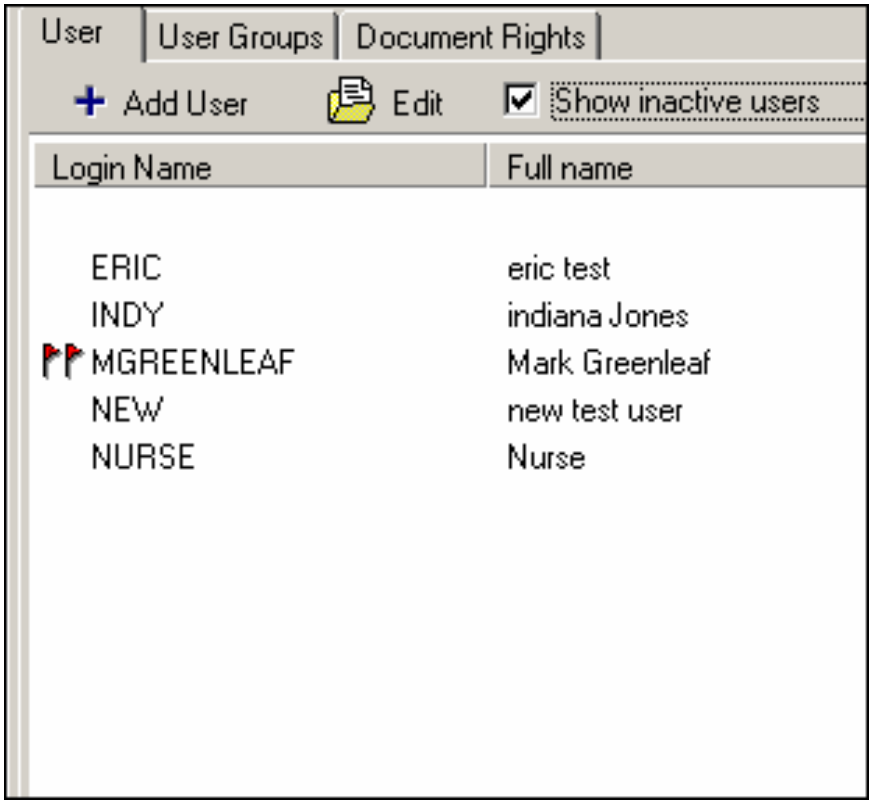


Figure 24

The Active box is unchecked.

10. Check the **Active** box
11. Click OK

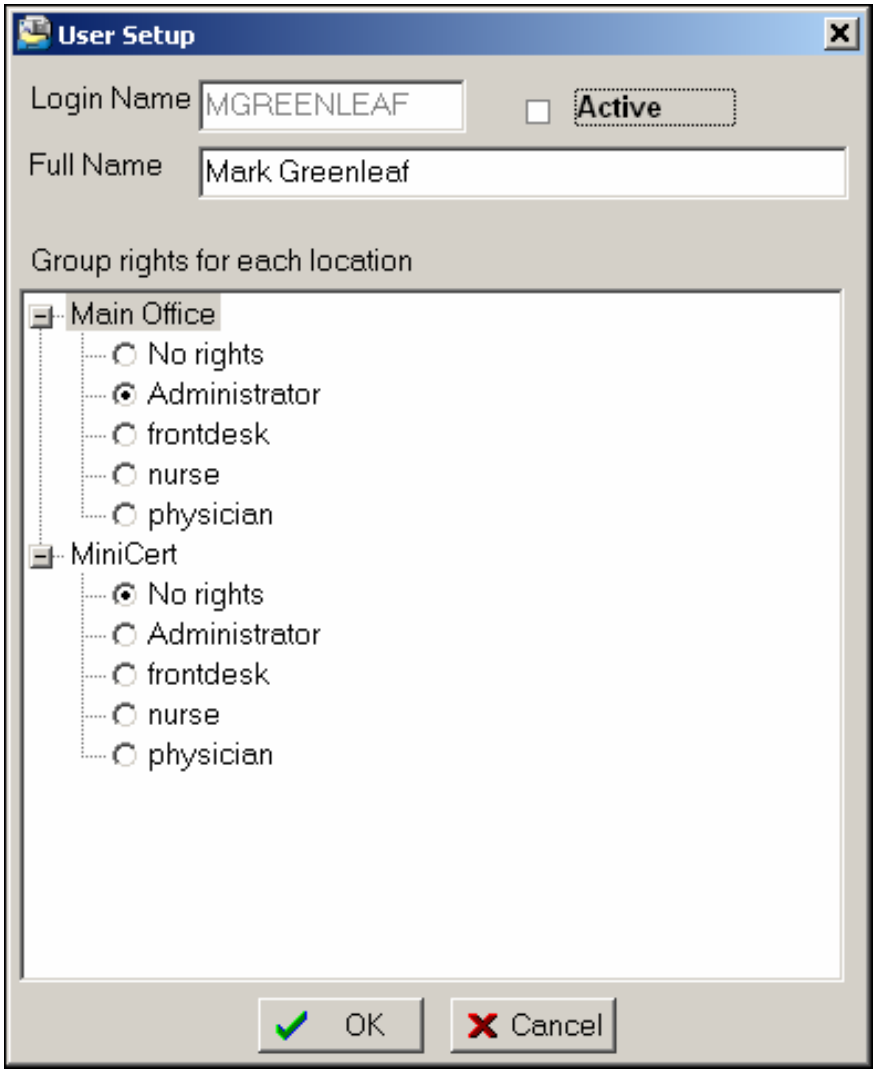


Figure 25

The user MGREENLEAF is reactivated.

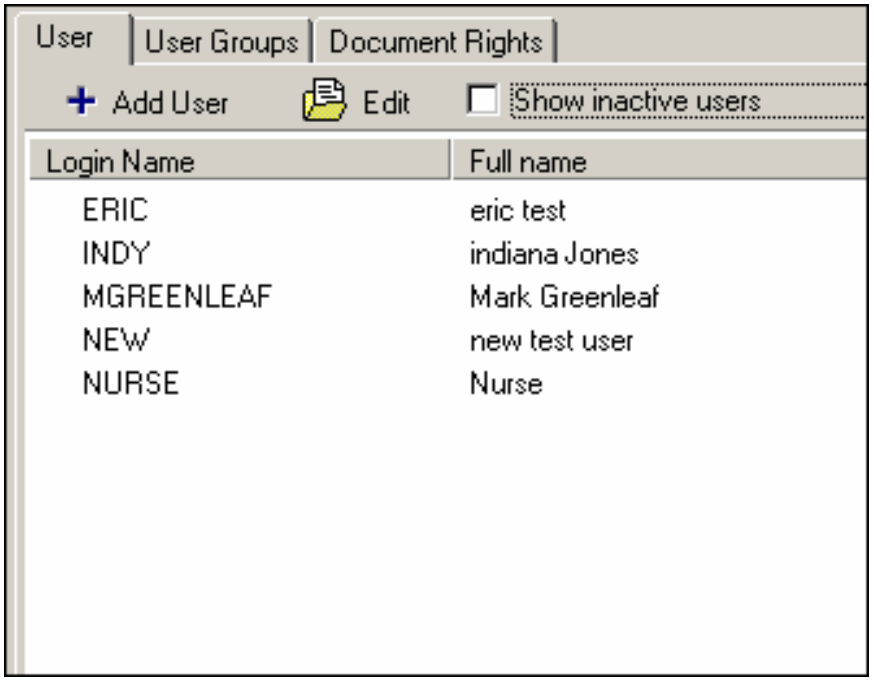


Figure 26

Passwords

Managing passwords and defining criteria is quick and easy.

1. Open the **Criterions TCMS Practice Management System**
2. Click **File -> Setup** (Figure 1).

Note: A user must have administrative rights to access the Practice Management Setup.

The Practice Setup Options List will appear.

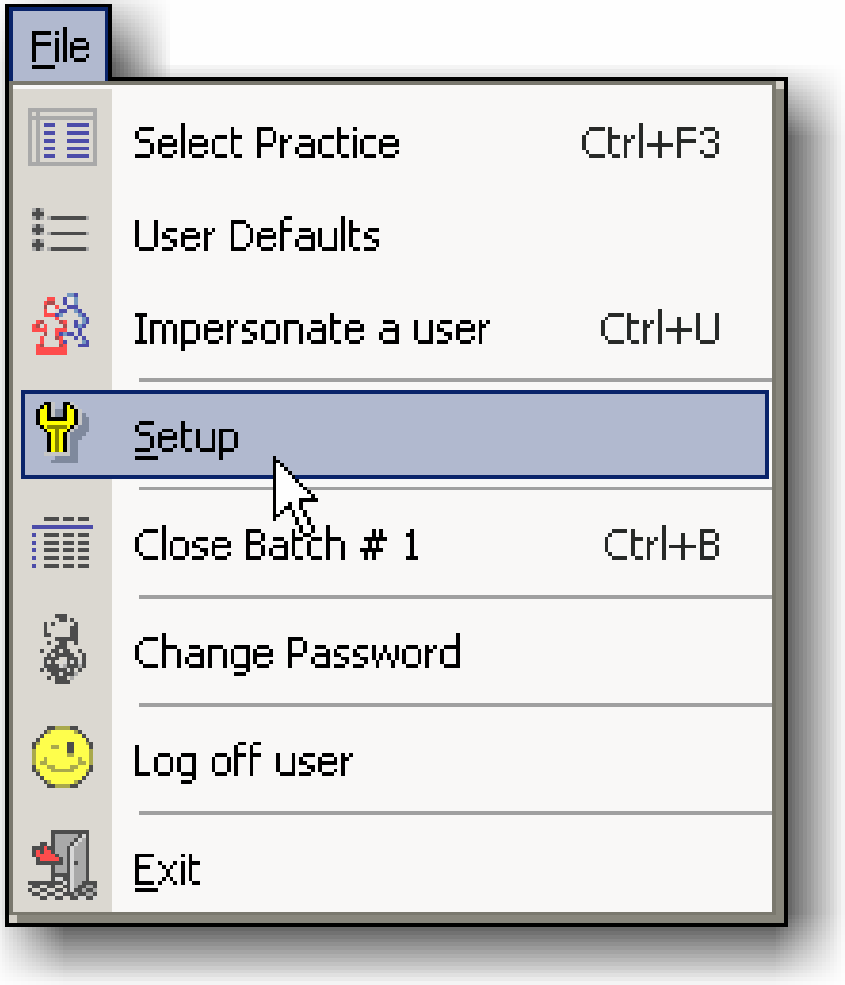


Figure 27

1. Select **Practice Setup -> User Setup.**
2. Select the **Password Rule Setup**.

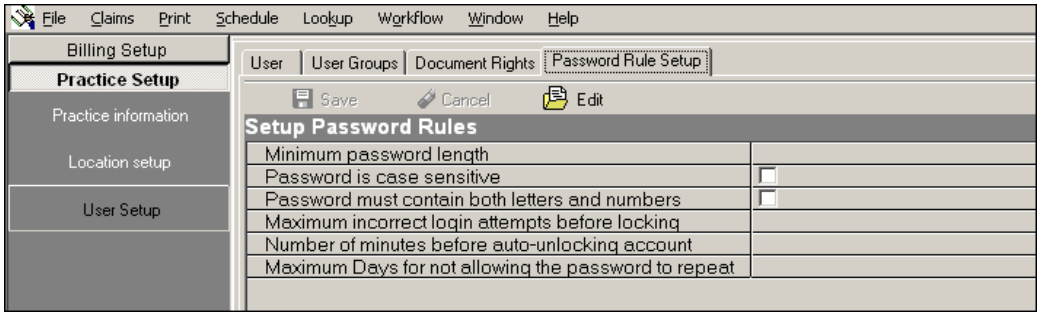


Figure 28

All practice password setup options are available from this screen.

3. Click

.

Note: Changes to the Password Rule Setup screen are applied to ALL users of the Practice Management and EHR systems.

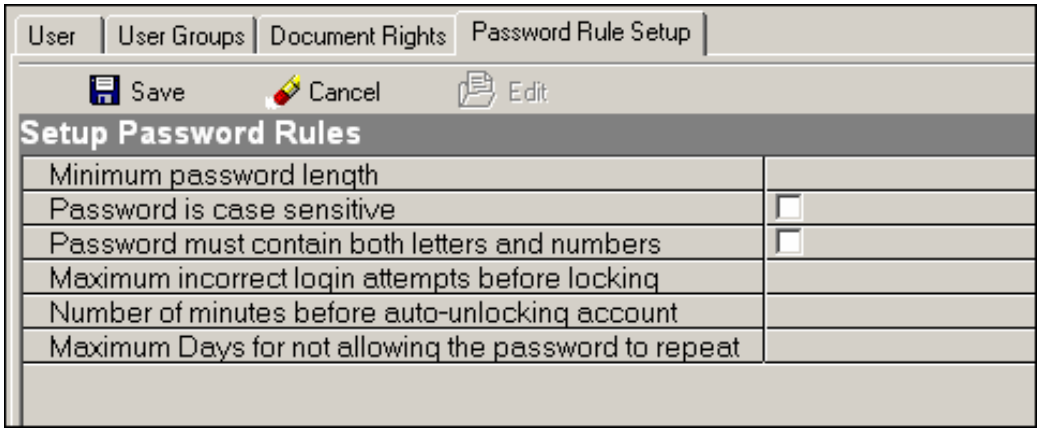


Figure 29

System administrators can define the minimum length to which user passwords must adhere.

4. Click in the box right of the "**Minimum password length**" field.
5. Enter the number for the minimum password length.

Note: Alpha characters are not accepted in this field. The field is limited to two numeric characters.

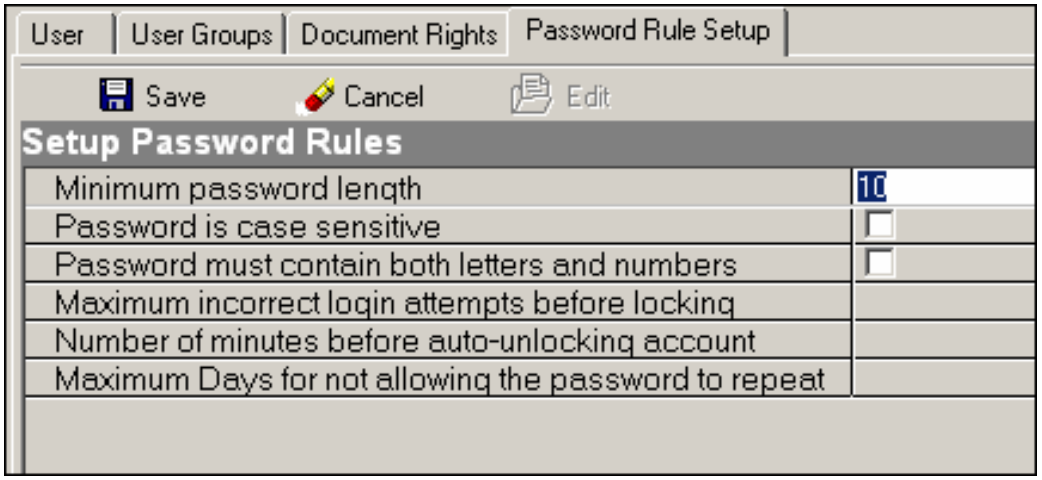


Figure 30

System administrators can set criteria that define passwords as case sensitive and/or requiring passwords to contain both letters and numbers.

6. Click the check box next to the "**Password is Case Sensitive field**".
7. Click the check box next to the "**Password must contain both letters and numbers**" field.

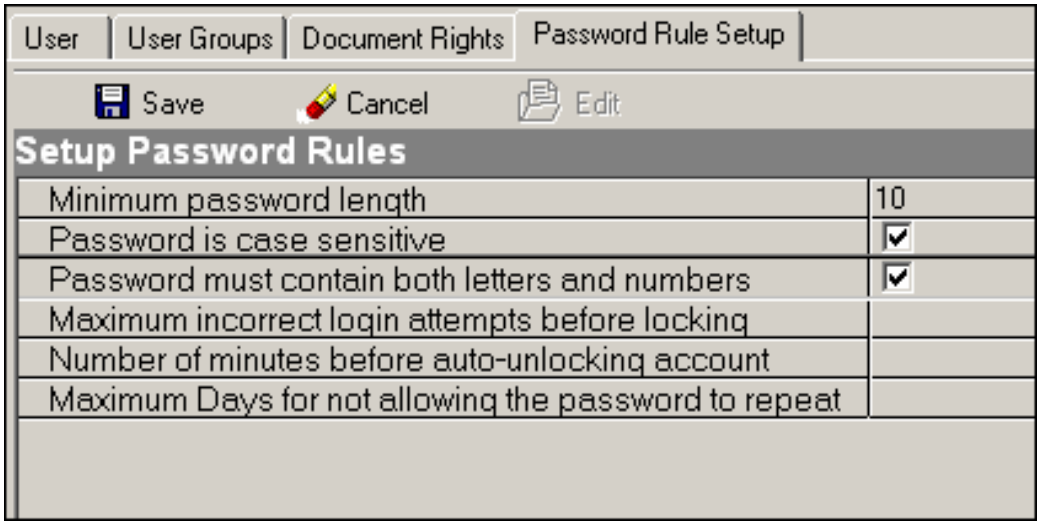


Figure 31

System administrators can define the number of incorrect login attempts that can be made before the user account is locked.

8. Click in the box right of the "**Maximum incorrect login attempts before locking"** field.
9. Enter the number for the maximum incorrect login attempts.

Note: Alpha characters are not accepted in this field. The field is limited to one numeric character.

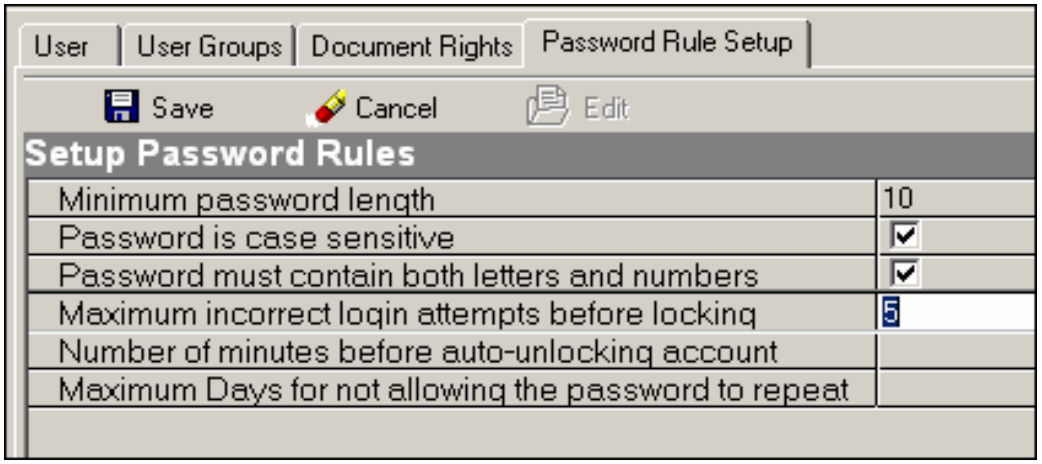


Figure 32

System administrators can define the number of minutes before a locked account will automatically unlock and accept repeated attempts.

10. Click in the box right of the "**Number of minutes before auto-unlocking account"** field.
11. Enter the number minutes before auto-unlocking account.

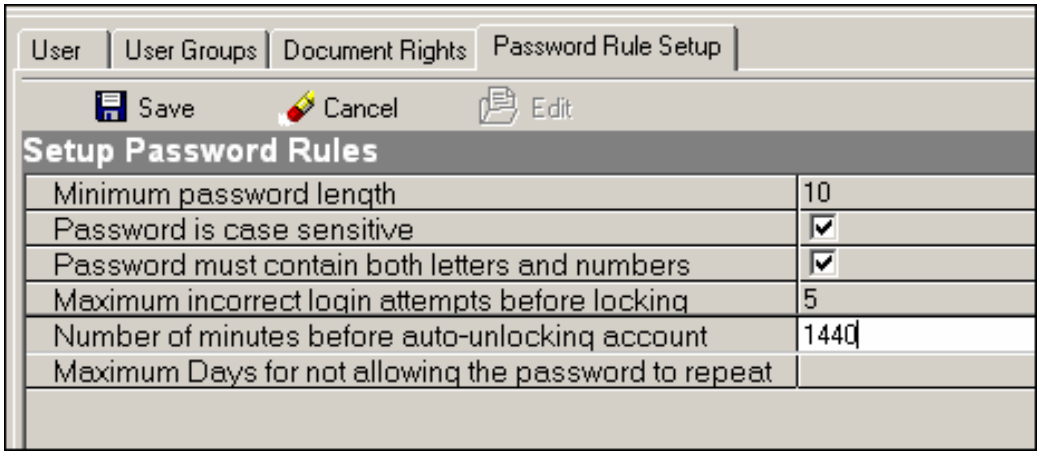


Figure 33

Note: Alpha characters are not accepted in this field. The field is limited to four numeric characters.

Note: 24 hours = 1440 minutes

System administrators can define the number of days that are required to pass before a password may be reused.

12. Click in the box right of the "**Maximum Days for not allowing the password to repeat**" field.
13. Enter the number days required before a password may be reused.

Note: Alpha characters are not accepted in this field. The field is limited to three numeric characters.

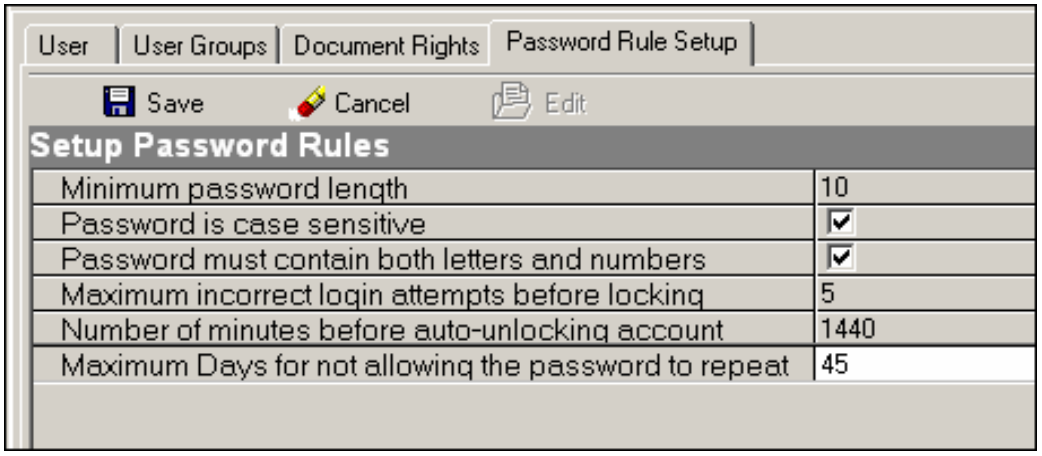


Figure 34

14. Once all password requirements have been defined, click Save

A pop-up box will appear notifying the administrator that the changes made will force all users to reset their passwords at their next login.

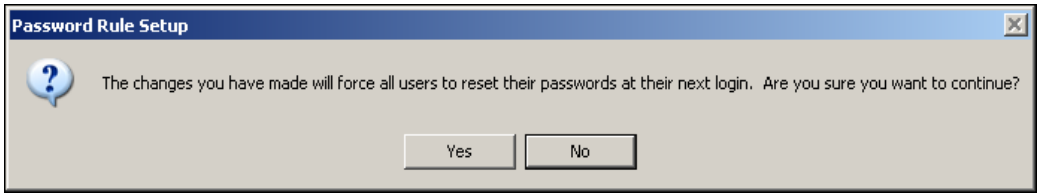

Password Rule Setup
The changes you have made will force all users to reset their passwords at their next login. Are you sure you want to continue?
Yes
No

Figure 35

15. Click Yes.

Admin Reset of Passwords

If a user account is locked or the password needs to be reset for any reason, log into the practice management setup to access a user account.

1. Open the **Criterions TCMS Practice Management System**
2. Click **File -> Setup** (Figure 1).

Note: A user must have administrative rights to access the Practice Management Setup.

The Practice Setup Options List will appear.

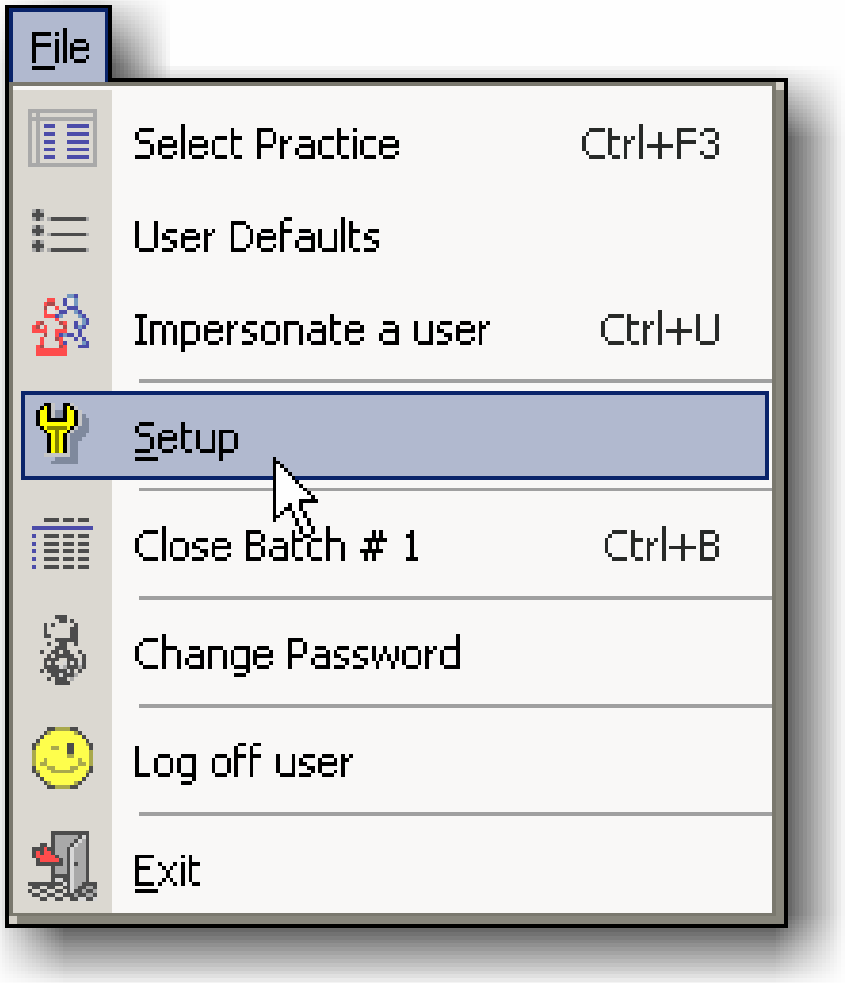


Figure 36

3. From the Setup menu, click **Practice Setup** (Figure 3).
4. Click **User Setup.**

Figure 37

A list of active user accounts is displayed.

5. Double-Click on the name of the user you would like to reset the password for.

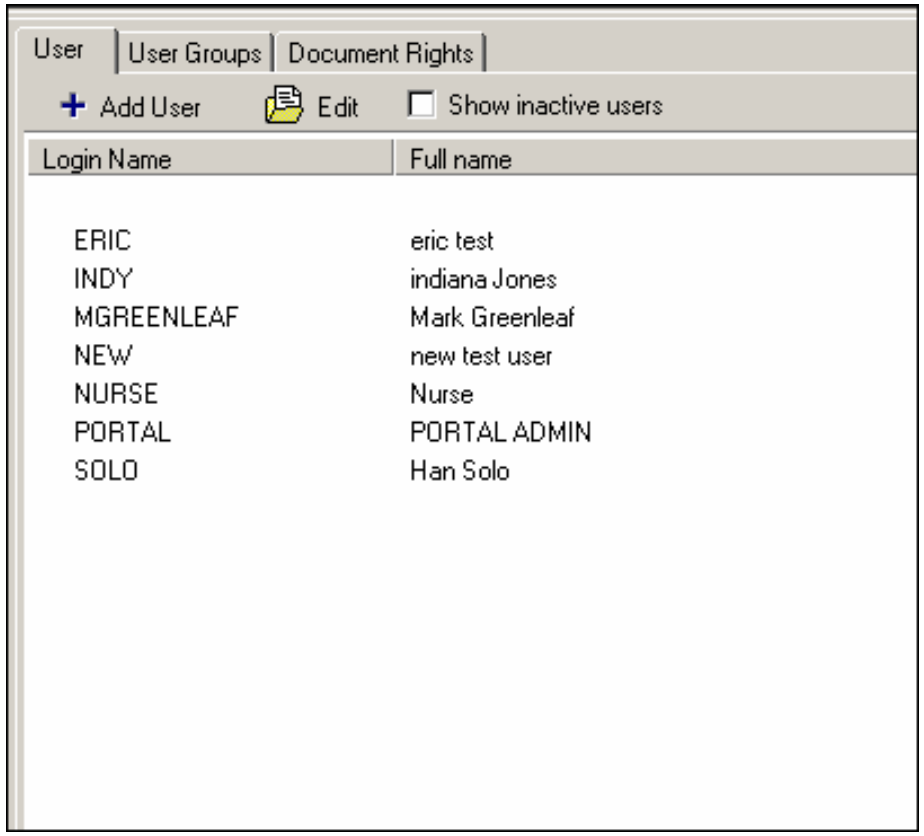


Figure 38

System administrators can force the reset of a user's password.

6. Check the box next to Reset Password.
7. Click OK.

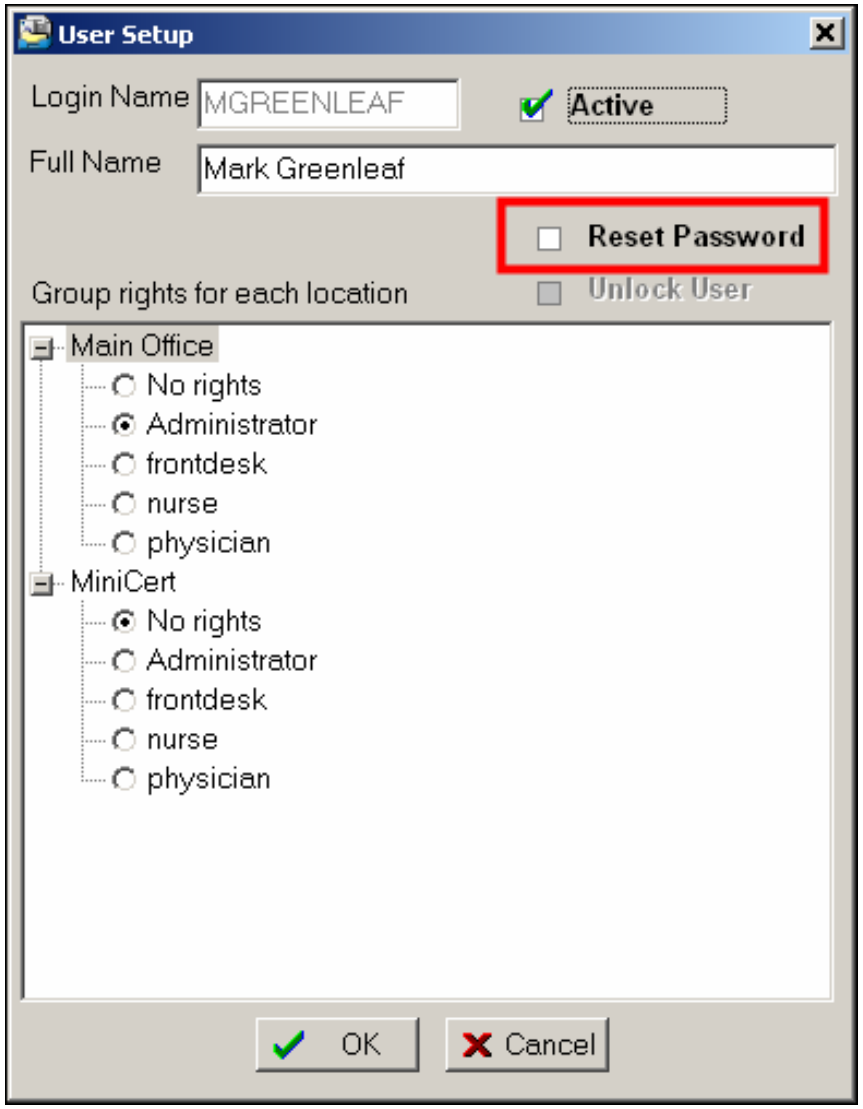


Figure 39

The system will ask the administrator to confirm the action.

8. Click Yes.

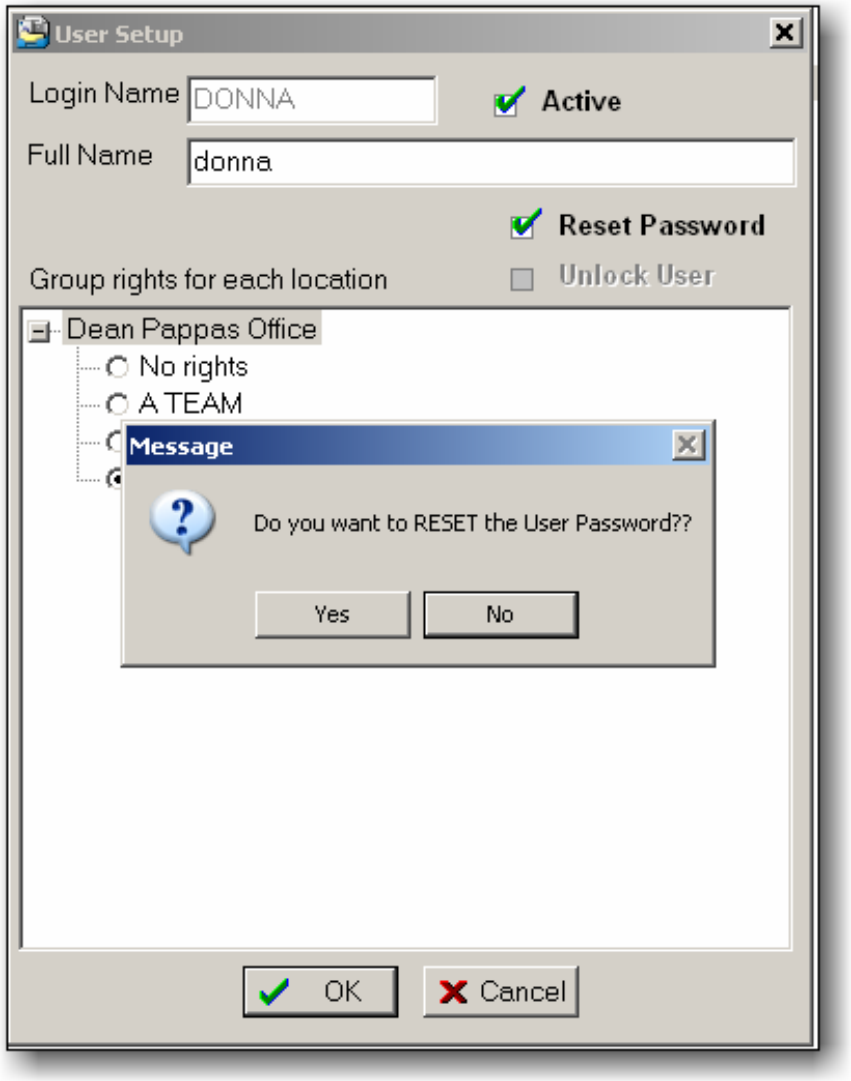


Figure 40

Upon login the user will receive the following prompt: "*Your Password has been reset by the Aministrator. Please enter a new password*."

9. Click

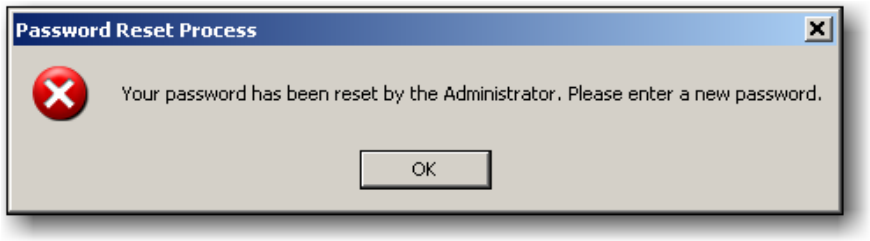


Figure 41

The user will be asked for a new password.

Figure 42

Administrative Unlocking of Accounts

After a user fails to enter the correct combination of user name and password past the allowed number of attempts the account will become locked.

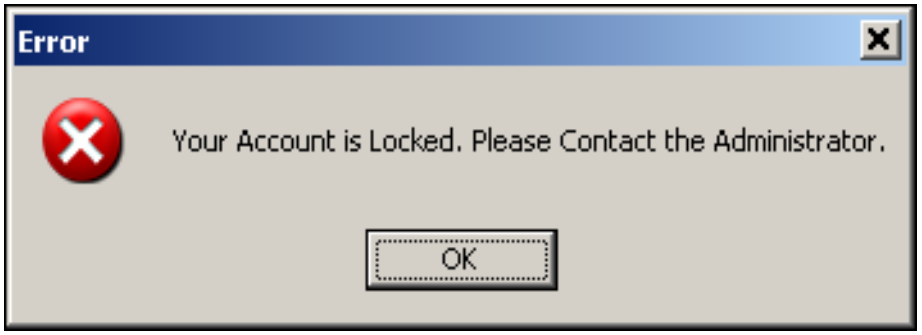


Figure 43

The administrator has rights to unlock a patient account.

1. Open the **Criterions TCMS Practice Management System**
2. Click **File -> Setup** (Figure 1).

Note: A user must have administrative rights to access the Practice Management Setup.

The Practice Setup Options List will appear.

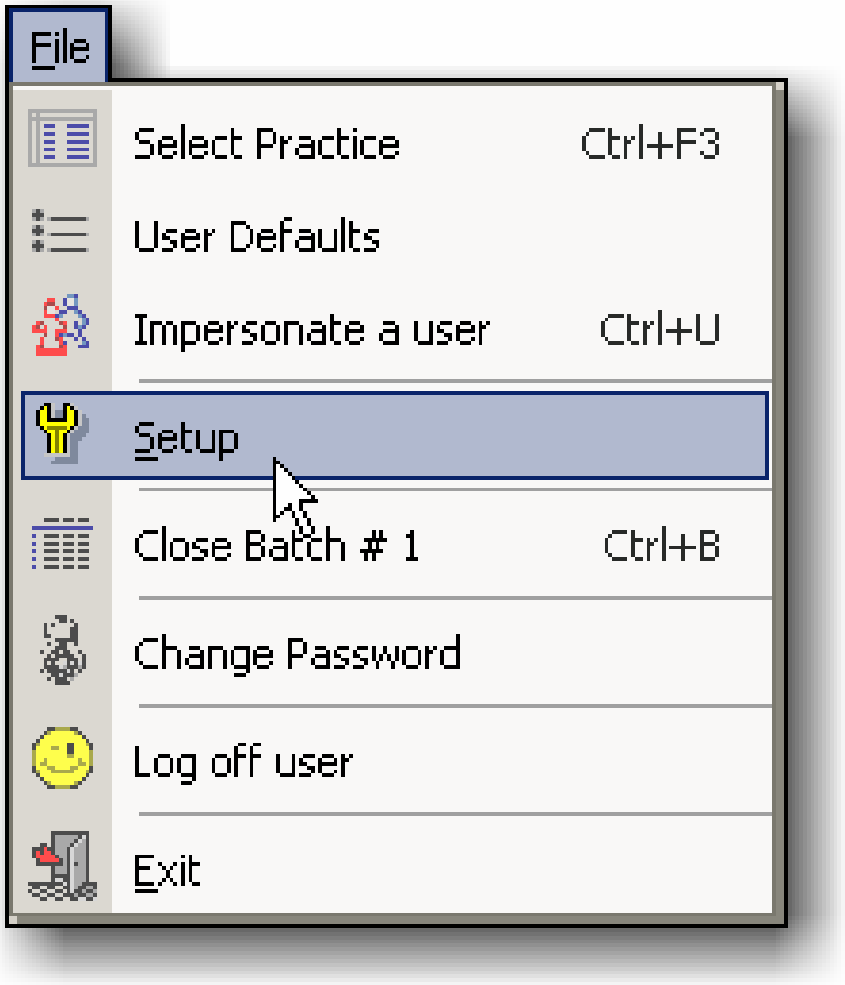


Figure 44

3. From the Setup menu, click **Practice Setup** (Figure 3).
4. Click **User Setup.**

Figure 45

A list of active user accounts is displayed. User accounts that are locked will show a lock icon next to the name.

5. Double-Click on the name of the account you would like to unlock.

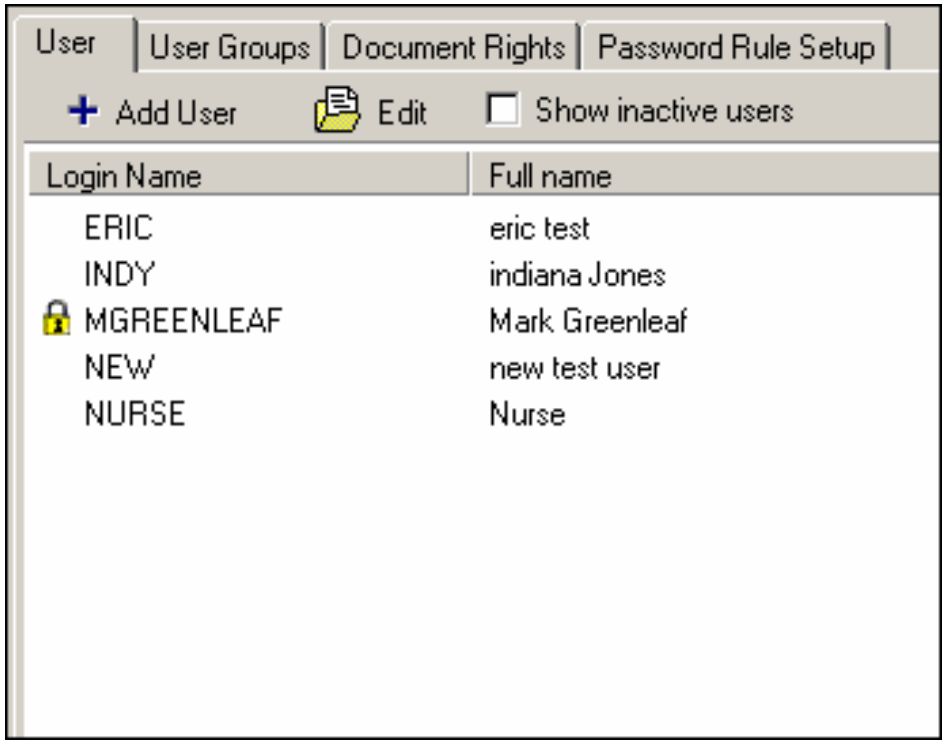


Figure 46

The user setup page will appear. The "Unlock User" field is now active.

6. Check the box next to Reset Password.
7. Click OK.

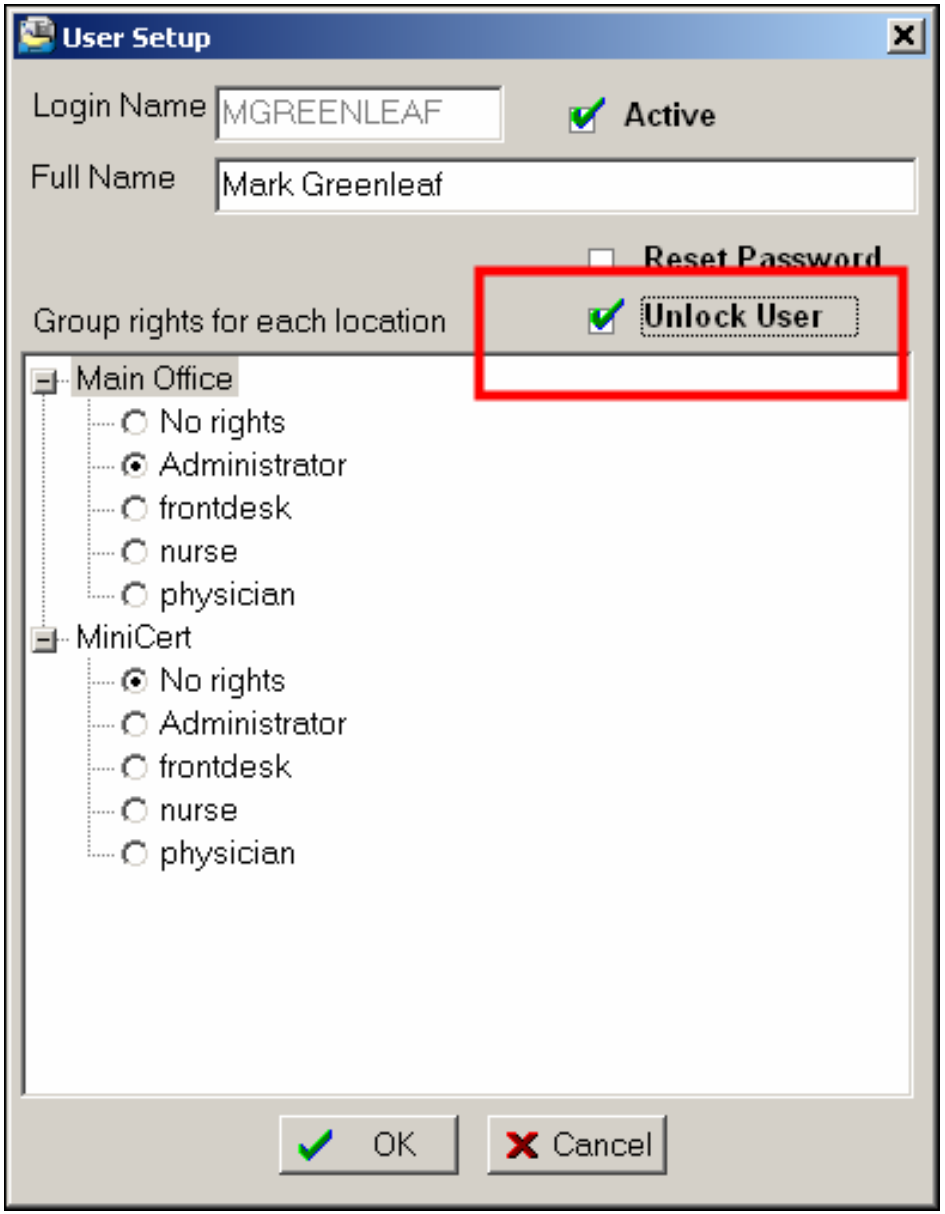


Figure 47

A pop-up will appear to confirm that the user wants to unlock the account.

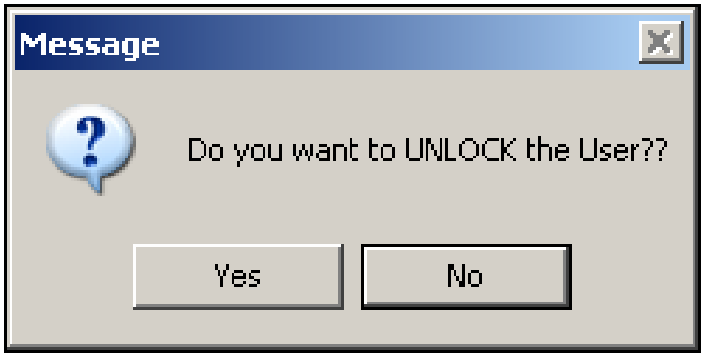


Figure 48

8. Click Yes.

The user account is unlocked. The user can now attempt to log in again.

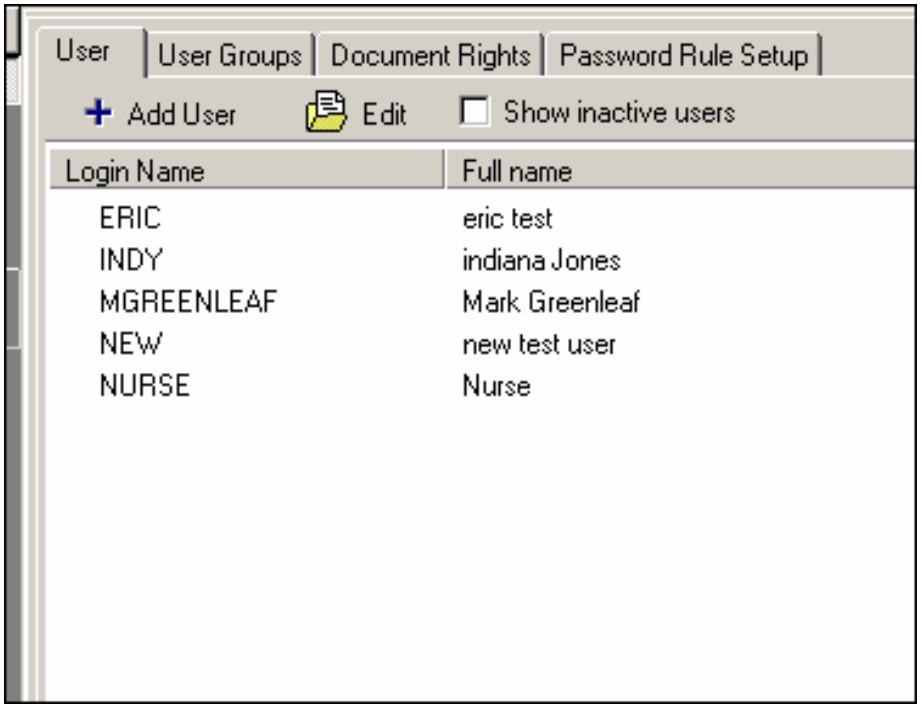


Figure 49

Incorrect User Attempts

Attempts to reuse a password prior to the limit being reached will result in an error message displayed to the user.

Figure 50

If a password has been reset by the administrator the user will be required to enter a new password, then retype the new password upon next login.

Figure 51

Criteria of the new password is displayed on the pop-up box.

The user will be presented with errors if they incorrectly attempt to reset their password.

Figure 52

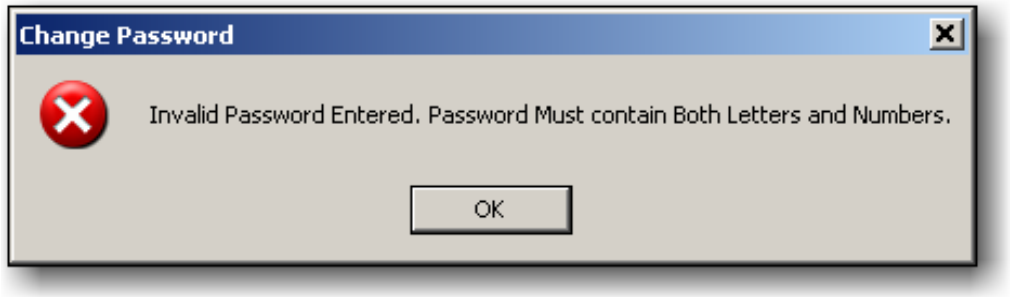


Figure 53

Figure 54

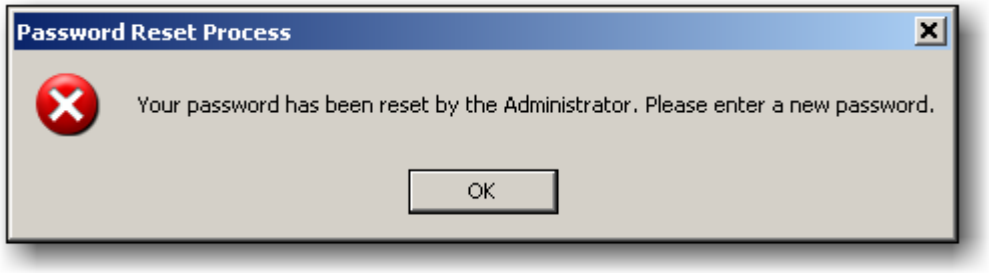


Figure 55

Accessing Audit Logs

Access to audit logs are a group right. To give a group rights you must have rights to access the practice management setup.

The administrator has rights to unlock a patient account.

1. Open the **Criterions TCMS Practice Management System**
2. Click **File -> Setup** (Figure 1).

Note: A user must have administrative rights to access the Practice Management Setup.

The Practice Setup Options List will appear.

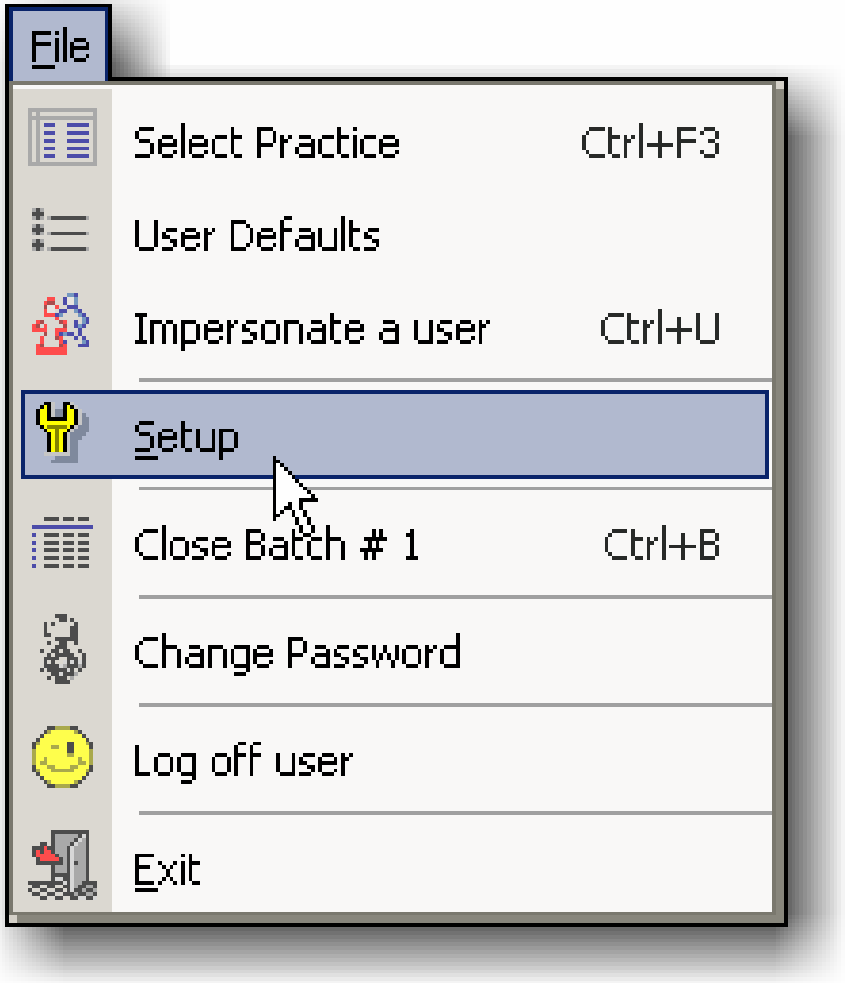


Figure 56

3. From the Setup menu, click **Practice Setup** (Figure 3).
4. Click **User Setup.**

Figure 57

To give audit rights the admin must edit the User Group.

5. Click on the **USER GROUPS** tab.

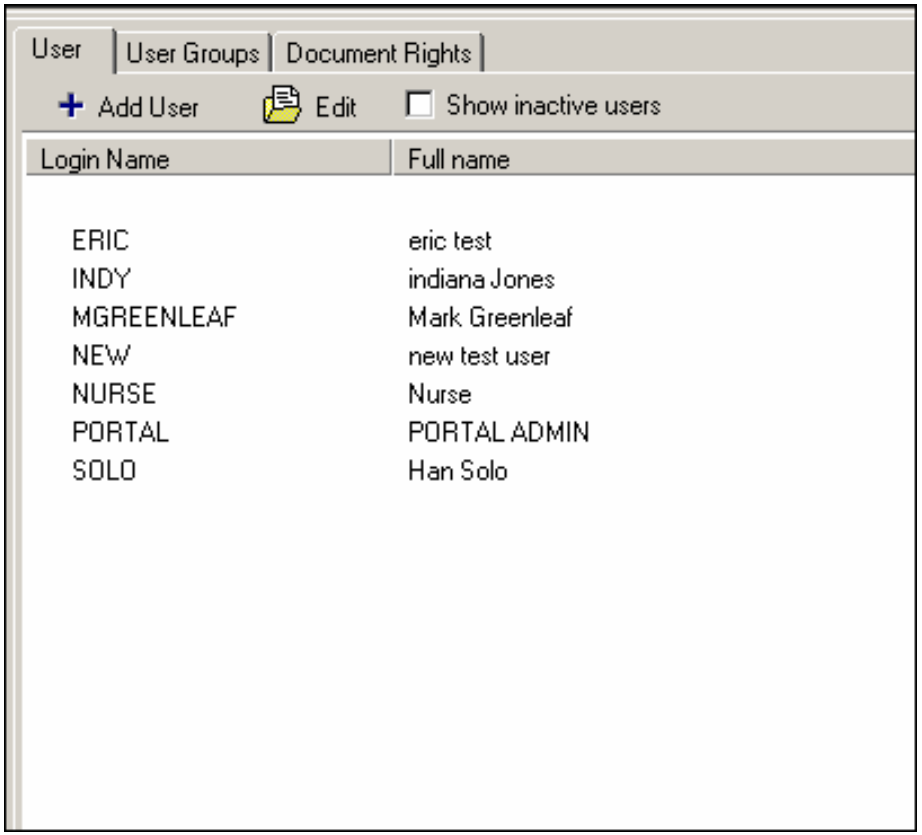


Figure 58

The added group names display in the left hand column.

6. Click on the **GROUP NAME** you would like to give audit log rights.

In this example, we are editing the rights for the Frontdesk group.

A list of group rights displays.

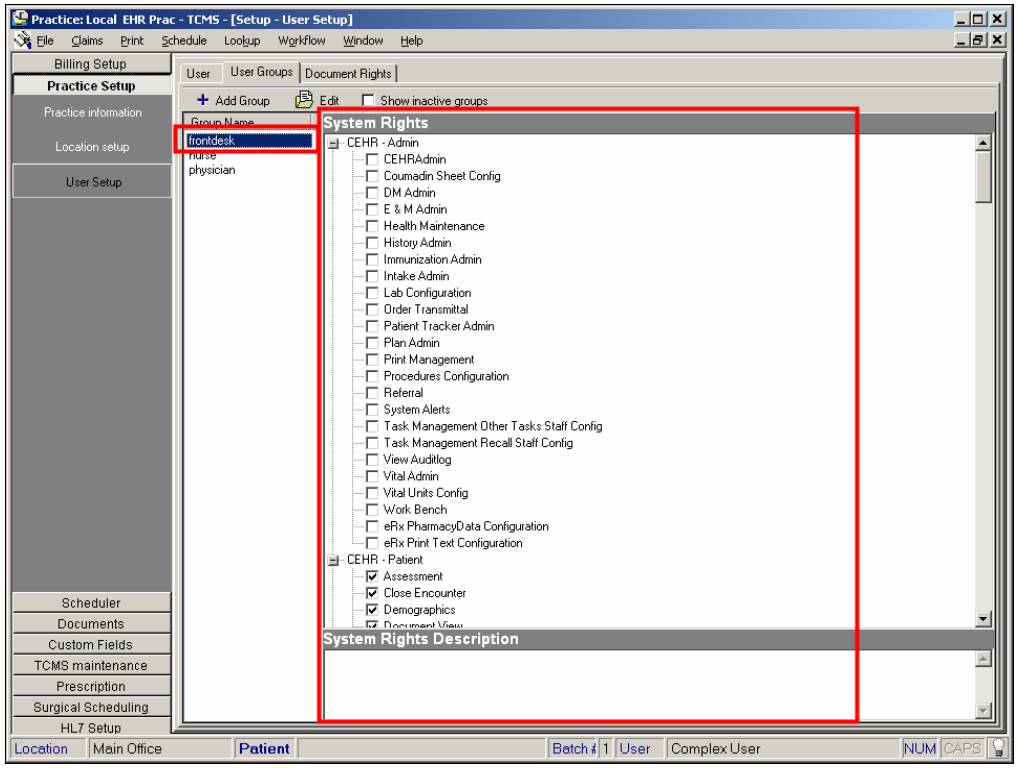


Figure 59

7. Scroll down to find the right you want to edit.

In this scenario insurance card Viewing Audit Log rights are to be given to all members of the front desk group.

8. Check the box before "View Auditlog."

All users across all locations who are given *Frontdesk* group rights will now have the ability to view the auditlogs.

If a user is a member of a group and needs rights that should not be given to the additional group members, a new group should be added and the user moved to that group.

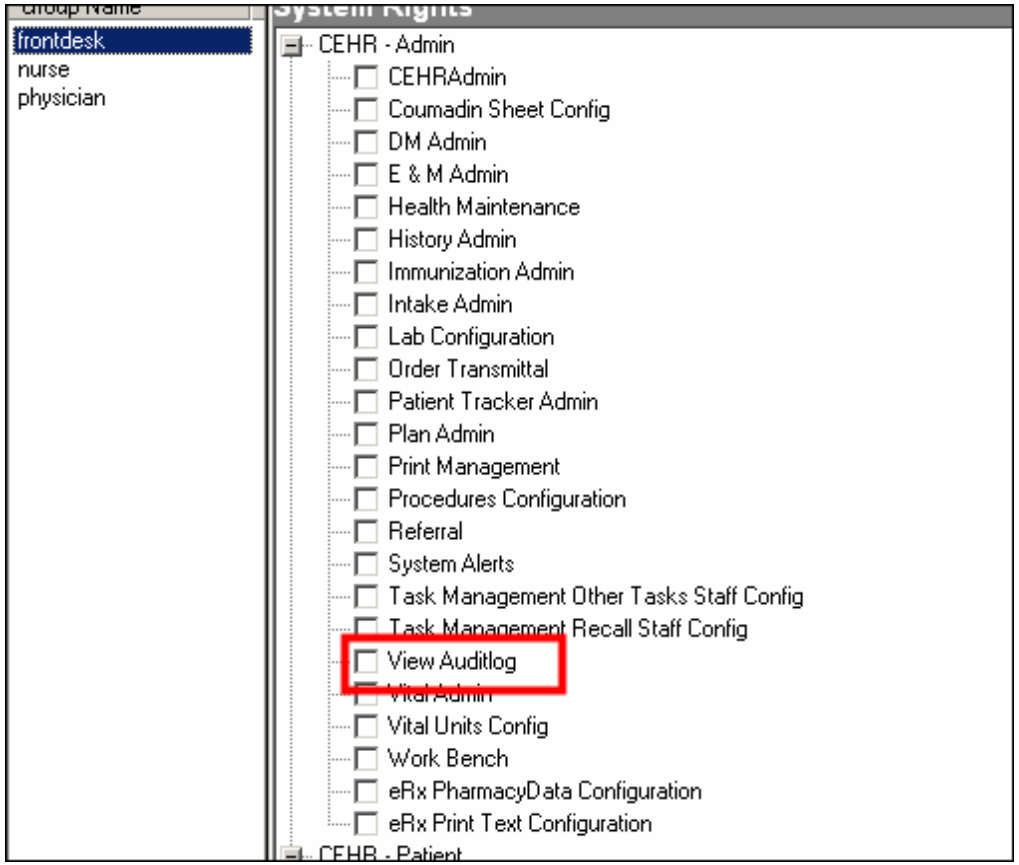


Figure 60

Audit logs are separated into two categories: Patient and Practice Audit Logs.

Practice Audit Logs:

If rights are granted to a user they can view audit logs within the admin section of the EHR.

9. In the EHR click

.

The admin menu will display.

10. Click the **User Security** link.

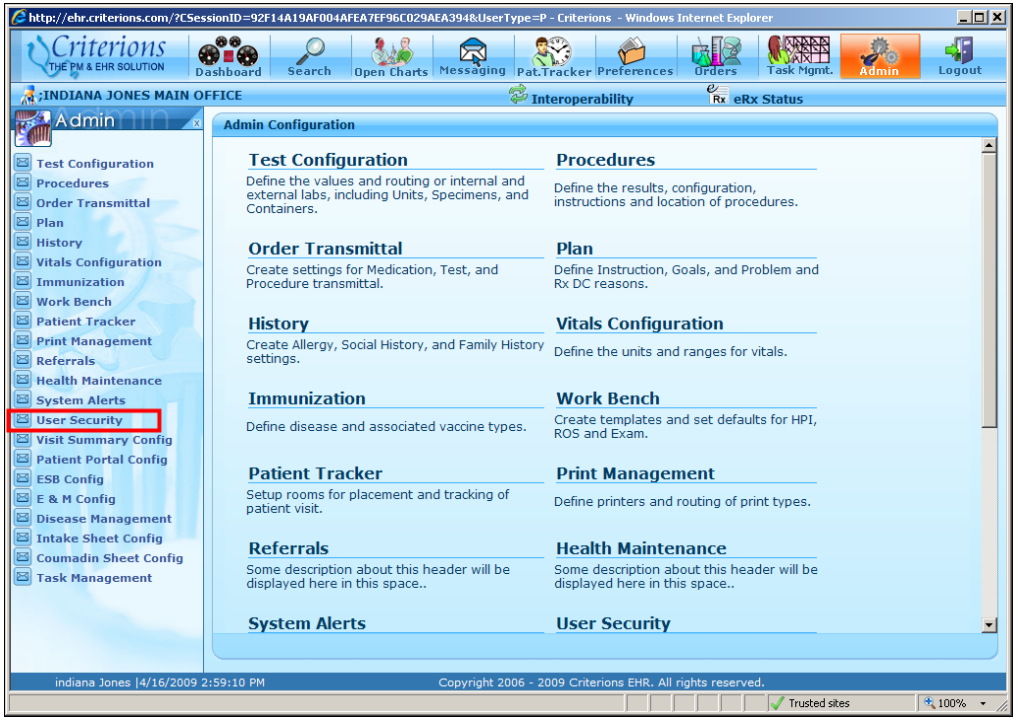


Figure 61

The list of user security options is displayed.

11. Click on the **User Login Audit** link.

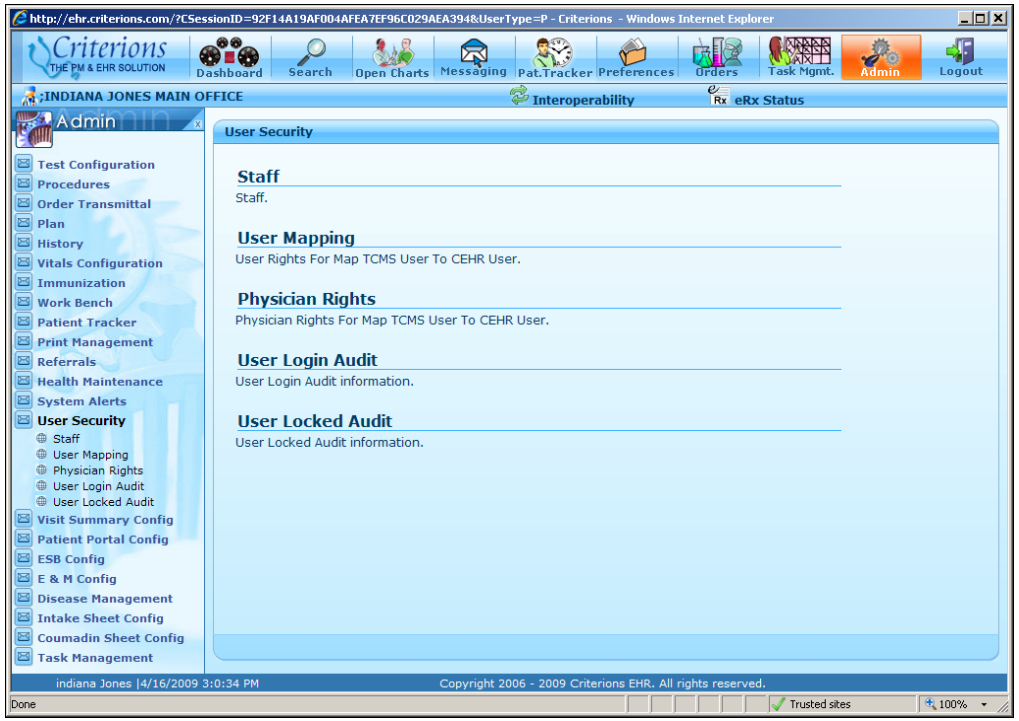


Figure 62

The User Login audit log is displayed. The user login audit log allows a user to perform a filtered search by user, start date or end date.

Each entry is date/time stamped with login and logout time.

12. Click on the **User Locked Audit** link.

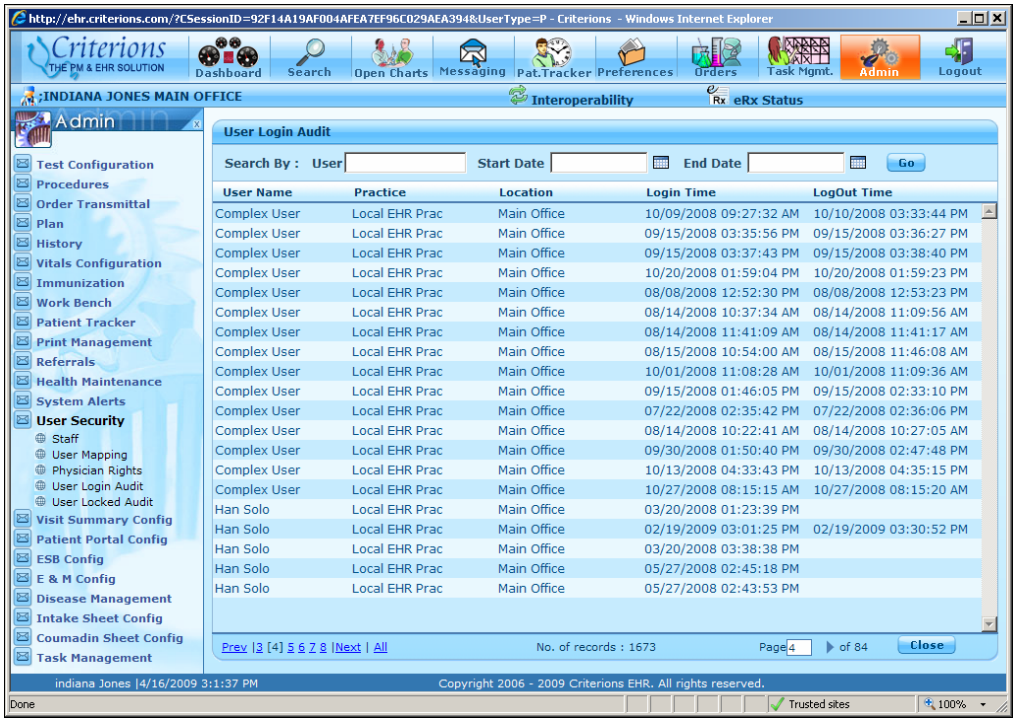

http://ehr.criterions.com/?CSessionID=92F14A19AF004AFEA7EF96C029AEA394&UserType=P - Criterions - Windows Internet Explorer
Criterions THE PM & EHR SOLUTION
Dashboard
Search
Open Charts
Messaging
Pat.Tracker
Preferences
Orders
Task Mgmt.
Admin
Logout
INDIANA JONES MAIN OFFICE
Interoperability
eRx Status
Admin
Test Configuration
Procedures
Order Transmittal
Plan
History
Vitals Configuration
Immunization
Work Bench
Patient Tracker
Print Management
Referrals
Health Maintenance
System Alerts
User Security
Staff
User Mapping
Physician Rights
User Login Audit
User Locked Audit
Visit Summary Config
Patient Portal Config
ESB Config
E & M Config
Disease Management
Intake Sheet Config
Coumadin Sheet Config
Task Management
User Login Audit
Search By : User
Start Date
End Date
Go
User Name | Practice | Location | Login Time | LogOut Time
Complex User | Local EHR Prac | Main Office | 10/09/2008 09:27:32 AM | 10/10/2008 03:33:44 PM
Complex User | Local EHR Prac | Main Office | 09/15/2008 03:35:56 PM | 09/15/2008 03:36:27 PM
Complex User | Local EHR Prac | Main Office | 09/15/2008 03:37:43 PM | 09/15/2008 03:38:40 PM
Complex User | Local EHR Prac | Main Office | 10/20/2008 01:59:04 PM | 10/20/2008 01:59:23 PM
Complex User | Local EHR Prac | Main Office | 08/08/2008 12:52:30 PM | 08/08/2008 12:53:23 PM
Complex User | Local EHR Prac | Main Office | 08/14/2008 10:37:34 AM | 08/14/2008 11:09:56 AM
Complex User | Local EHR Prac | Main Office | 08/14/2008 11:41:09 AM | 08/14/2008 11:41:17 AM
Complex User | Local EHR Prac | Main Office | 08/15/2008 10:54:00 AM | 08/15/2008 11:46:08 AM
Complex User | Local EHR Prac | Main Office | 10/01/2008 11:08:28 AM | 10/01/2008 11:09:36 AM
Complex User | Local EHR Prac | Main Office | 09/15/2008 01:46:05 PM | 09/15/2008 02:33:10 PM
Complex User | Local EHR Prac | Main Office | 07/22/2008 02:35:42 PM | 07/22/2008 02:36:06 PM
Complex User | Local EHR Prac | Main Office | 08/14/2008 10:22:41 AM | 08/14/2008 10:27:05 AM
Complex User | Local EHR Prac | Main Office | 09/30/2008 01:50:40 PM | 09/30/2008 02:47:48 PM
Complex User | Local EHR Prac | Main Office | 10/13/2008 04:33:43 PM | 10/13/2008 04:35:15 PM
Complex User | Local EHR Prac | Main Office | 10/27/2008 08:15:15 AM | 10/27/2008 08:15:20 AM
Han Solo | Local EHR Prac | Main Office | 03/20/2008 01:23:39 PM
Han Solo | Local EHR Prac | Main Office | 02/19/2009 03:01:25 PM | 02/19/2009 03:30:52 PM
Han Solo | Local EHR Prac | Main Office | 03/20/2008 03:38:38 PM
Han Solo | Local EHR Prac | Main Office | 05/27/2008 02:45:18 PM
Han Solo | Local EHR Prac | Main Office | 05/27/2008 02:43:53 PM
Prev |3 [4] 5 6 7 8 |Next | All
No. of records : 1673
Page 4 of 84
Close
indiana Jones |4/16/2009 3:1:37 PM
Copyright 2006 - 2009 Criterions EHR. All rights reserved.
Done
Trusted sites
100%

Figure 63

The user Locked Audit will display the lock and unlock date/time for each lock event. The user who unlocked the account is also displayed.

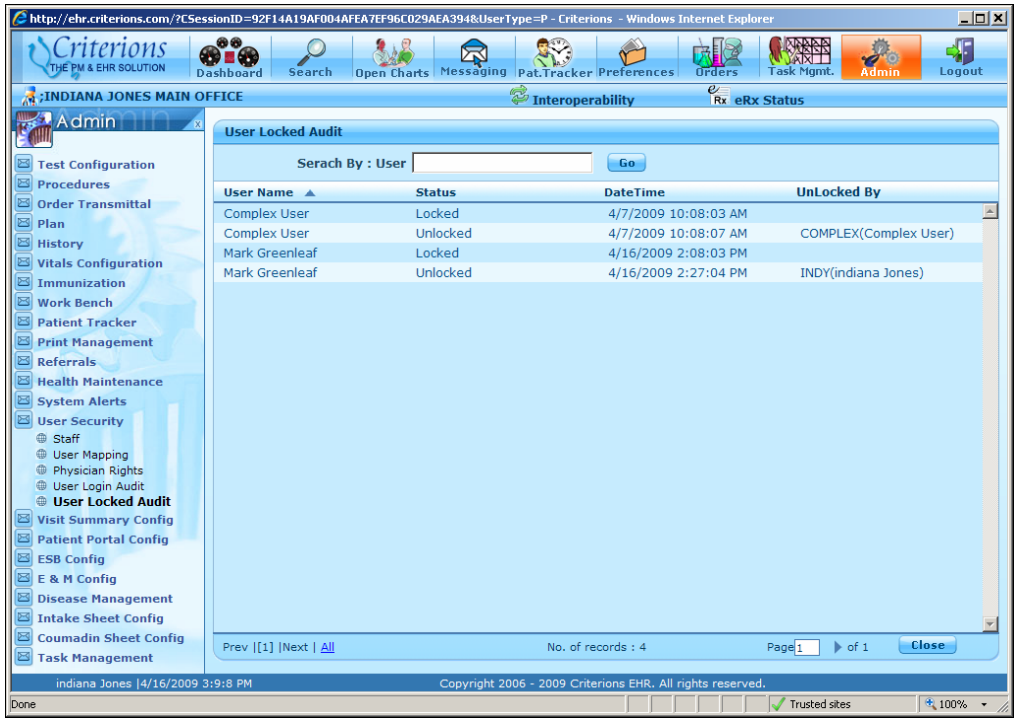


Figure 64

Patient Audit Logs:

Audit Logs involving patient records are displayed within the patient record.

13. Click

to search for a patient.
14. Enter the patient name or account.
15. Click

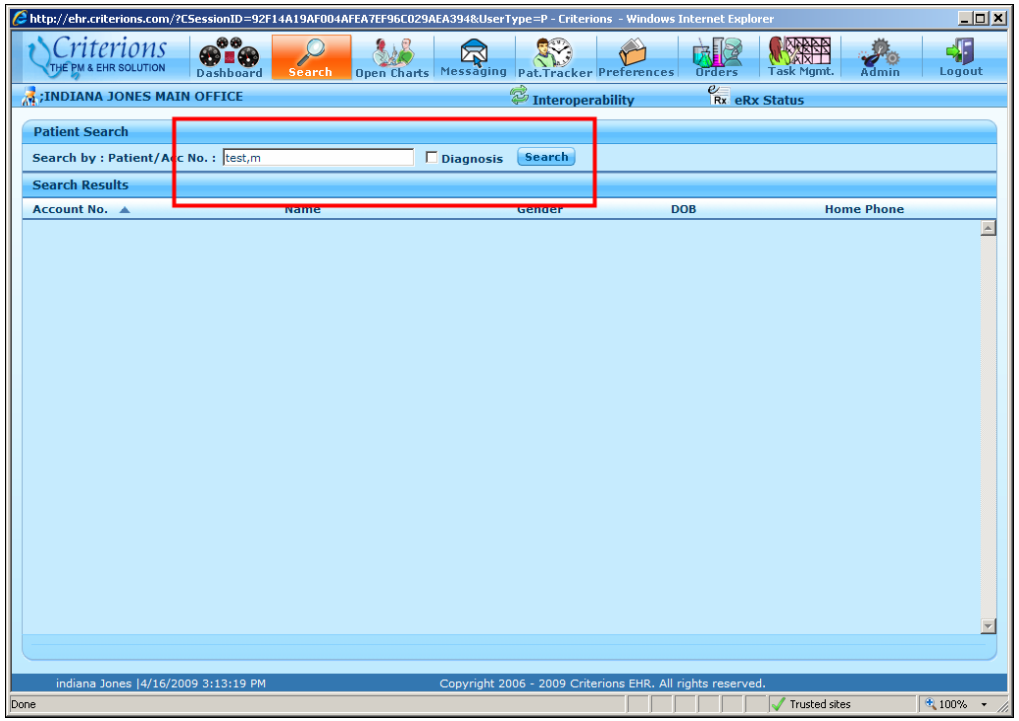


Figure 65

A list of patients matching the search criteria will display.

16. Select the patient by clicking on their name.

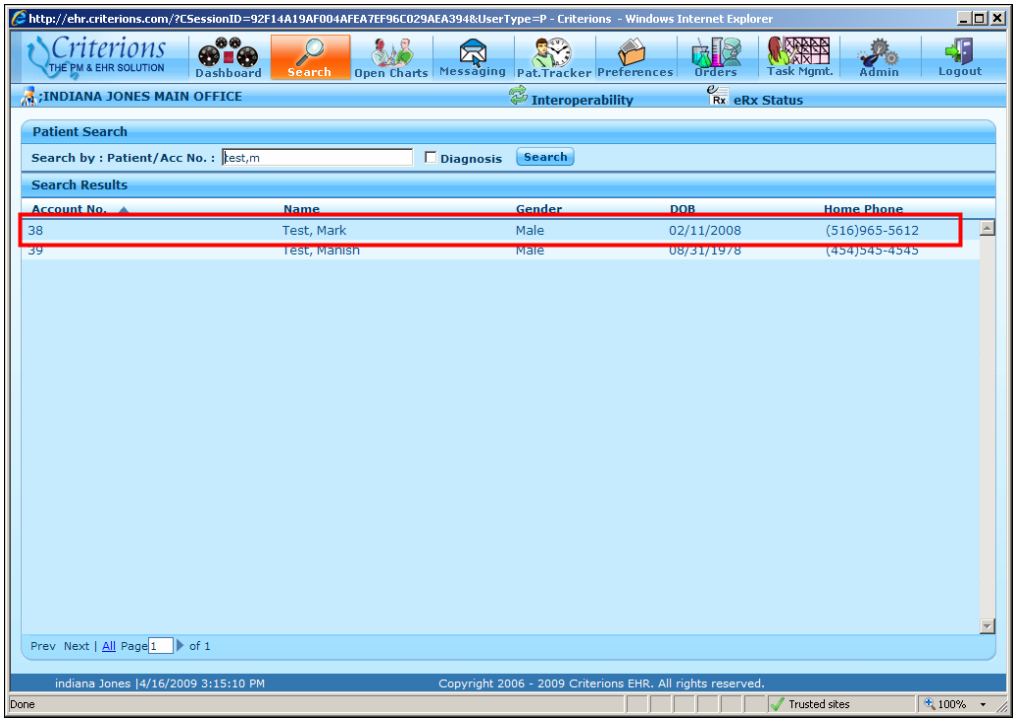


Figure 66

The patient chart is opened.

Because audit logs record information changed in the course of a visit or outside of a visit we store audit logs at a visit level. The audit log will display audit information pertaining to the visit as well as information independent of the visit.

17. Click on a **PRIOR VISIT.**

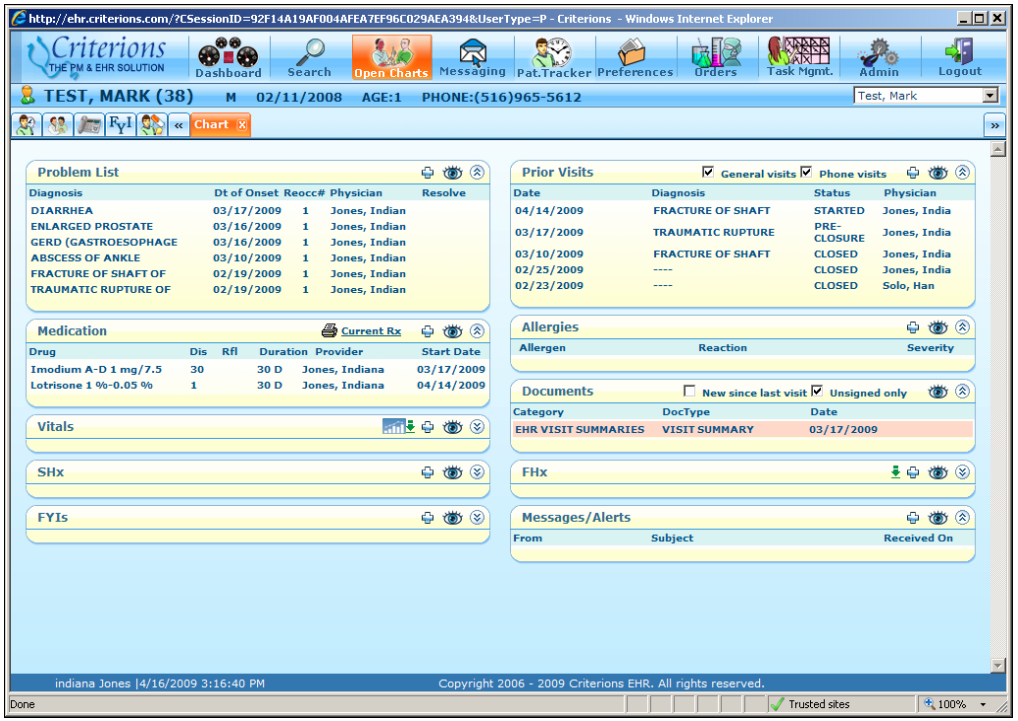


Figure 67

The patient visit is displayed.

18. Click

to display the audit information.

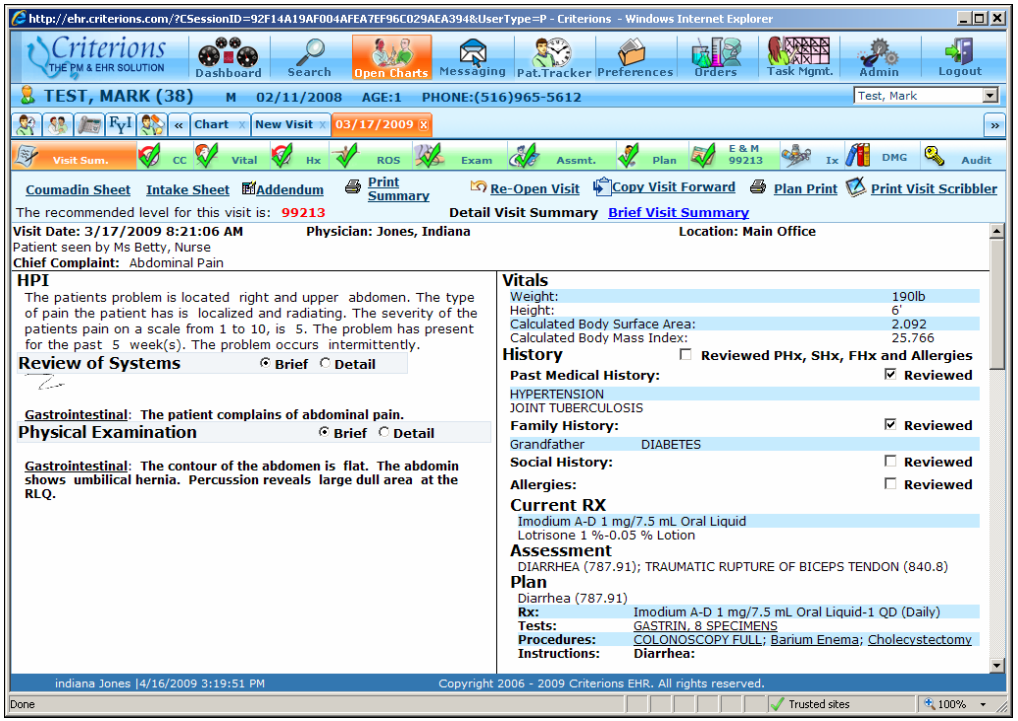


Figure 68

All items pertaining to the patient record and the visit are accessible.

By default the Visit Audit log displays.

This screen records who has changed any status (Open, Close, Started, Reopened) to the visit.

A list of additional filters is displayed on the left hand side. Links on the top half pertain to items that are separate from a particular visit. The items in the lower half of the screen are visit specific audit logs.

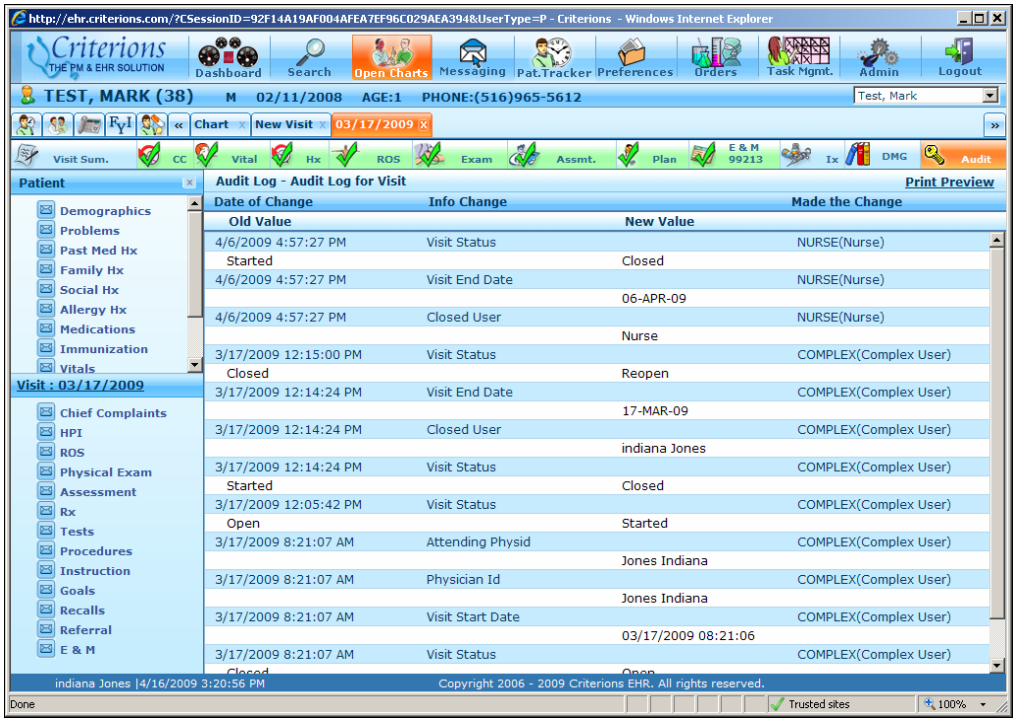


Figure 69

19. Click the link for **Pat Chart Access**.

A list of all users who have accessed the patient chart at any time is displayed.

Any list in the audit log can be printed.

20. Click the **Print Preview** link.

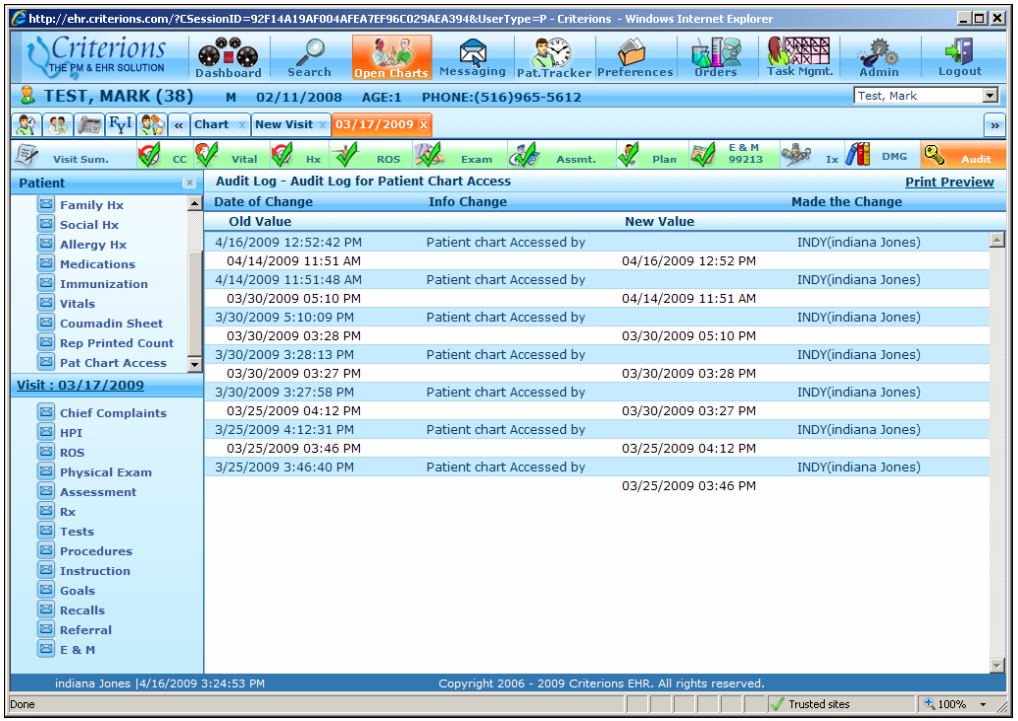


Figure 70

A preview of the printout is viewed.

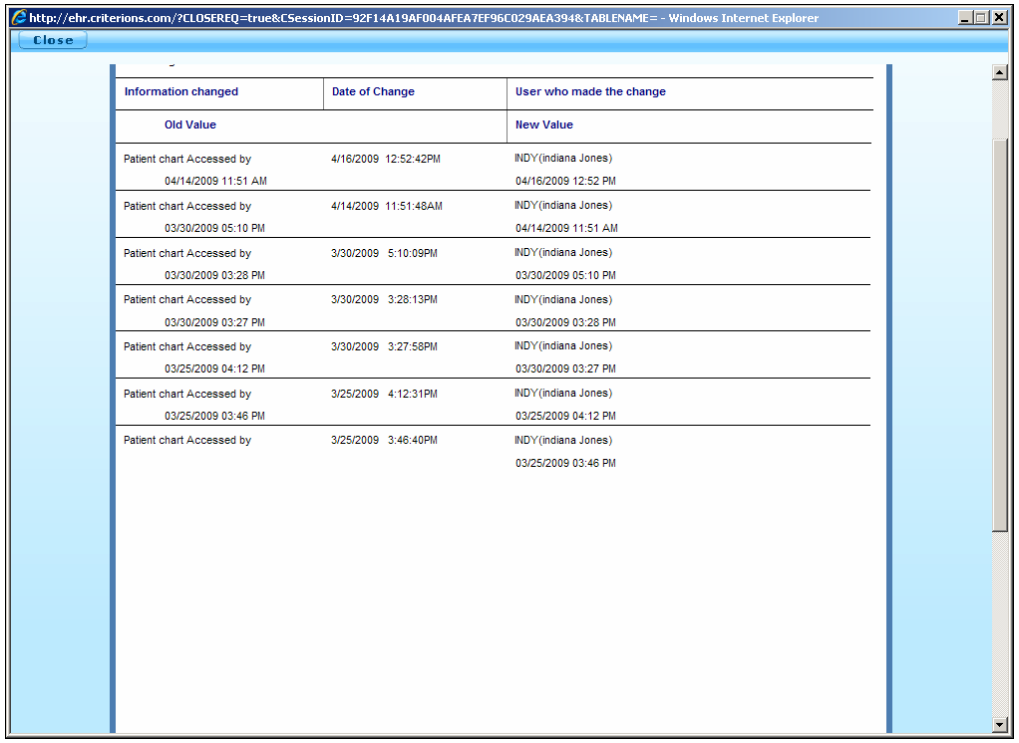

http://ehr.criterions.com/?CLOSEREQ=true&CSessionID=92F14A19AF004AFEA7EF96C029AEA394&TABLENAME= - Windows Internet Explorer
Close
Information changed
Date of Change
User who made the change
Old Value
New Value
Patient chart Accessed by 04/14/2009 11:51 AM 4/16/2009 12:52:42PM INDY(indiana Jones) 04/16/2009 12:52 PM
Patient chart Accessed by 03/30/2009 05:10 PM 4/14/2009 11:51:48AM INDY(indiana Jones) 04/14/2009 11:51 AM
Patient chart Accessed by 03/30/2009 03:28 PM 3/30/2009 5:10:09PM INDY(indiana Jones) 03/30/2009 05:10 PM
Patient chart Accessed by 03/30/2009 03:27 PM 3/30/2009 3:28:13PM INDY(indiana Jones) 03/30/2009 03:28 PM
Patient chart Accessed by 03/25/2009 04:12 PM 3/30/2009 3:27:58PM INDY(indiana Jones) 03/30/2009 03:27 PM
Patient chart Accessed by 03/25/2009 03:46 PM 3/25/2009 4:12:31PM INDY(indiana Jones) 03/25/2009 04:12 PM
Patient chart Accessed by 3/25/2009 3:46:40PM INDY(indiana Jones) 03/25/2009 03:46 PM

Figure 71

A print button is located in the upper left corner.

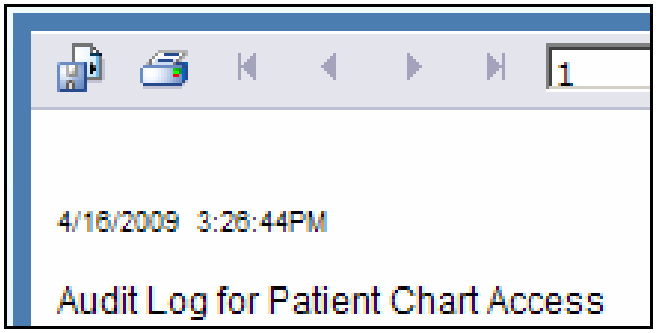


Figure 72

Contact

For clarification of any part of this document or policies regarding Criterions or our products, please contact us at 516.466.1942 or info@criterions.com